REDEFINING SECURITY

a report by the

Joint Security Commission

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 28021994	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Redefining Security	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Joint Security Commission Washington, D.C. 20505	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms "IATAC COLLECTION"	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 173	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	2/1/95	Report

4. TITLE AND SUBTITLE
Redefining Security

5. FUNDING NUMBERS

6. AUTHOR(S)
Joint Security Commission

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis
Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

The report describes the threats to our nation’s security and lays out a vision the Joint Security Commission believes will shift the course of security philosophy. It also proposes a new policy structure and a classification system designed to manage risks better, and outlines methods of improving government and industry personnel security policies. This report offers recommendations on developing new strategies for achieving security within our infor-mation systems, including protecting the integrity and availability of both classified and unclassifiedinformation assets.

14. SUBJECT TERMS
IA

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

REDEFINING SECURITY

A Report to the
Secretary of Defense
and the
Director of Central Intelligence

February 28, 1994

Joint Security Commission
Washington, D.C. 20505

Joint Security Commission
Washington, D.C. 20505

February 28, 1994

The Honorable William J. Perry
Secretary of Defense
Pentagon
Washington, D. C. 20301

The Honorable R. James Woolsey
Director of Central Intelligence
Washington, D. C. 20505

Dear Sirs:

1. Pursuant to your request, the Joint Security Commission was convened on June 11, 1993. The Commission was guided by your direction to develop a new approach to security that would "assure the adequacy of protection within the contours of a security system that is simplified, more uniform, and more cost effective."

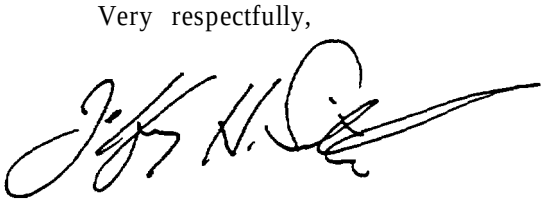
2. This report presents the recommendations of the Joint Security Commission to achieve these objectives and to redefine security policies, practices and procedures. The report describes the threats to our nation's security and lays out a vision the Commission believes will shift the course of security philosophy. We also propose a new policy structure and a classification system designed to manage risks better, and we outline methods of improving government and industry personnel security policies. We offer recommendations on developing new strategies for achieving security within our information systems, including protecting the integrity and availability of both classified and unclassified information assets, and we call for a new approach to capture security costs. We provide recommendations for linking traditional physical and technical countermeasures to threat. We believe that implementation of these recommendations will result in a security system that will meet the evolving threat while being fairer, more coherent, and more cost effective.

3. In reaching its conclusions and recommendations, the Commission drew upon the perspectives of policymakers, Congress, the military, industry, and public interest groups. Although our charter was limited to a review of the Intelligence and Defense Communities, we found that many of the problems and solutions have government-wide implications. In those instances where we believe that a government-wide solution is the best answer, we have offered recommendations to that effect.

4. This report represents months of work by the Commissioners, our staff, and a vast number of citizens both in and out of government, who graciously gave us their time and comments. On behalf of the Commission, I would like to thank all who contributed to this effort and to give special recognition to our superb staff, headed so ably by Dan Ryan. Ultimately, of course, the Commissioners bear full responsibility for the analysis and recommendations contained herein.

5. As you have directed, the Commission will remain in place until June 1, to assist in the implementation of our recommendations. We look forward to working with you to achieve the objectives you have laid before us.

Very respectfully,



Jeffrey H. Smith
Chairman

Attachment

Executive Summary

The world has changed dramatically during the last few years, with profound implications for our society, our government, and the Defense and Intelligence Communities. Our understanding of the range of issues that impact national security is evolving. Economic and environmental issues are of increasing concern and compete with traditional political and military issues for resources and attention. Technologies, from those used to create nuclear weapons to those that interconnect our computers, are proliferating. The implications and impacts of these technologies must be assessed. There is wide recognition that the security policies, practices, and procedures developed during the Cold War must be changed. Even without the end of the Cold War, it is clear that our security system has reached unacceptable levels of inefficiency, inequity, and cost. This nation must develop a new security system that can meet the emerging challenges we face in the last years of this century and the first years of the next.

With these imperatives in mind, the Joint Security Commission has focused its attention on the processes used to formulate and implement security policies in the Department of Defense and the Intelligence Community. In reviewing all aspects of security, the Commission has been guided by four principles:

- Our security policies and services must realistically match the threats we face. The processes we use to formulate policies and deliver services must be sufficiently flexible to facilitate change as the threat evolves.

- Our security policies and practices must be more consistent and coherent, thereby reducing inefficiencies and enabling us to allocate scarce resources effectively.

- Our security standards and procedures must result in the fair and equitable treatment of those upon whom we rely to guard the nation's security

- Our security policies, practices, and procedures must provide the needed security at a price the nation can afford.

The recommendations of the Commission, presented in detail in this report, fall mainly into three categories:

(1) recommendations that will maintain and hopefully enhance security, but at a lower cost by avoiding duplication and increasing efficiency;

(2) recommendations that will reduce current levels of security but in accordance with risk management principles based on a changing threat; and

(3) recommendations that will create new processes to formulate and oversee security policy govemmentwide.

In a very few cases-most notably concerning personnel security and information systems security-the Commission is recommending additional security requirements that will increase costs. The Commission's recommendations also include changes that are revenue neutral but will make the security system both more rational and inherently more fair. Although the Commission is recommending certain specific changes, the primary concern of the Commission is to create new and flexible processes that will adjust security policies, practices, and procedures to achieve our stated goals as the political, economic, and military realities evolve.

In the past, most security decisions have been linked one way or another to assumptions about threats. These assumptions frequently postulated an all-knowing, highly competent enemy. Against this danger, we have striven to avoid security risks by maximizing our defenses and minimizing our vulnerabilities. Today's threats are more diffuse, multifaceted, and dynamic. We also know that some vulnerabilities can never be eliminated fully nor would the costs and benefits warrant trying. While the Commission recognizes that the consequences of some security failures are exceptionally dire and require exceptional protection measures, in most cases it is possible to balance the risk of loss or damage of disclosure against the costs of countermeasures. We can then select a mix that provides adequate protection without excessive cost in dollars and without impeding the efficient flow of information to those who require ready access to it. The Commission believes that the nation must develop a security framework that will provide a rational, cost-effective, flexible set of policies, practices, and procedures. This framework must use a risk management approach that considers actual threats, inherent vulnerabilities, and the availability and costs of countermeasures as the underlying basis for making security decisions.

Risk management requires evaluating the resource impact of proposed changes in security policies and standards. This is practically impossible with today's accounting systems because they are not designed to collect security cost data. The Commission believes that establishing a system to capture security costs is crucial to effective streamlining and cost reduction. Therefore, we have recommended the creation of a uniform cost-accounting methodology and tracking system for security resources expended by the Department of Defense, the Intelligence Community, and supporting industry.

The Commission believes two areas require particular attention. First, personnel security lies at the very heart of our security system. No amount of physical, information systems, or procedural security will be sufficient if we cannot ensure the trustworthiness of those who must deal with sensitive and classified information. Grave damage has been caused to the United States by current or former employees and contractors of the government who decided to become spies for our adversaries. Therefore, the Commission believes that renewed efforts must be made to strengthen our personnel security system. The Commission also recognizes the necessity for enhancing the training we provide security officers, managers, and workers in the importance of security and of their roles in protecting the nation's information assets.

The processes we use to clear personnel in the Defense and Intelligence Communities vary widely from agency to agency. Different standards are

applied by different agencies; clearances are not readily transferable; and the time to grant a clearance ranges from a few weeks in one agency to months in others. Accordingly, we recommend common standards for adjudications and a joint investigative service to standardize background investigations and thus take advantage of economies of scale.

Second, information systems security requires increased attention. Productivity is, in today's world, directly related to information systems and their connectivity. The Defense and Intelligence Communities are increasingly dependent on information systems in performing their complex missions on behalf of the nation. Information systems technology is, however, evolving at a faster rate than information systems security technology. Overcoming the resulting gap will require careful threat assessments, well-thought-out investment strategies, sufficient funding, and management attention if our computers and networks are to protect the confidentiality, integrity, and availability of our classified and unclassified information assets.

The Commission believes that a systems approach is necessary in making decisions about the application of security countermeasures. By placing all the responsibility for security on each of the security disciplines, we have created requirements for multiple layers of security that add little value. This is particularly apparent in physical security, where classified documents may be stored in locked containers inside locked strong rooms within secure buildings in fenced facilities patrolled by armed guards-overkill even at the height of the Cold War, much less in today's security environment. A risk-managed systems approach would tailor countermeasures to threat and should result in significant savings that could be applied to improving personnel and information systems security, or to maintaining or improving other areas directly related to successful performance of defense and intelligence missions.

Nowhere will the payoff from improving our security policies, practices, and procedures be higher than in the industrial base supporting the Defense and Intelligence Communities. Our current practices subject industry to a bewildering array of requirements that are compliance-based, inconsistent, and often contradictory. Security requirements imposed on industry far exceed the requirements used by government agencies and organizations to protect the same information. While some budgetary and proprietary information must be withheld from some contractors in order to preserve competition, the Commission has found little reason to treat industry differently from government for security purposes. We must create a partnership between government and industry to enhance security, leaving adversarial roles behind. The Commission also believes that our security policies must not unnecessarily discourage foreign investment in American companies nor unduly burden our industrial base in competing for a larger share of the world's markets.

Central to the Commission's recommendations is the immediate formation of a single organization—a security executive committee chaired by the Secretary of Defense (or his designee) and the Director of Central Intelligence-responsible for the creation of security policies and overseeing the coherent implementation of those policies across the Defense and Intelligence Communities. This committee would not, of course, supplant the existing statutory authorities of the Secretary of Defense and the Director of Central Intelligence, including the latter's responsibility to protect sources and meth-

ods. This committee would, however, replace numerous existing fora that today independently develop security policies and procedures that are often inconsistent and are sometimes contradictory. A single source for security policies should result in reciprocity with consequential reductions in cost and improvements in efficiency. Although it is outside the scope of our charter, the Commission also believes that this committee should, in the very near future, be expanded by the addition of representatives from other government departments and agencies and given the responsibility to formulate governmentwide security policies. The committee, which should report to the National Security Council, should oversee the security system and have an outside advisory panel of distinguished Americana to ensure that industry, academia, and public interest groups have a voice in the formulation of security policies.

To facilitate the formulation, implementation, and oversight of security policies, practices, and procedures, the Commission proposes a radical new classification system that greatly simplifies the current system and eliminates the subjectivity inherent in it. The Commission worked closely with the Task Force revising Executive Order 12356 on National Security Information in analyzing possible changes and their impacts, and determined that a single level of classification with two degrees of protection should be adopted. Most classified information would be protected using a coherent set of personnel, physical, information systems, and procedural security standards and would be based on discretionary need-to-know as currently practiced for Confidential and Secret materials. Highly sensitive information, such as that protected at the Top Secret, Sensitive Compartmented Information, or Special Access Program levels today, would be protected by using a more stringent set of standards and would be based on centrally managed need-to-know determinations. Application of this system will be founded on risk management rather than complete avoidance of all risk and would concentrate on security as a service to our communities in place of the compliance-based, punitive approach in use today.

The Joint Security Commission is pleased to present its recommendations for the creation of an improved process for the formulation, management, and oversight of security policies, practices, and procedures. We believe that implementation of this process and the coherent application of its results should ensure that security countermeasures are chosen to match the evolving threat and that inefficiencies and costs are minim&d. The resulting security system would treat people fairly and provide a balanced mix of security needed to protect our information assets, facilities, personnel, and our nation's interests.

Joint Security Commission

Commissioners

Jeffrey H. Smith, ***Chairman***
Duane P. Andrews
J. Robert Burnett
Ann Caracristi
Antonia H. Chayes
Anthony A. Lapham
Nina J. Stewart
Richard F. Stolz
Harry A. Volz
Larry D. Welch

Staff

Dan J. Ryan, ***Executive Secretary***	CIA
John T. Elliff, ***Deputy Executive Secreta y***	DoD
Marisa Barthel	CIA
John E. Bloodsworth	CIA
Sheila Brand	NSA
Edmund Cohen	CIA
Rene Davis-Harding	DoD
Lee A. Falcon	DoD
Mary Griggs	DoD
Helmut H. Hawkins	DoD
Dan L. Jacobson	DoD
Richard P. Nyren, Jr.	DoD
Maria N. O'Connor	DoD
Michael D. Reynolds	CIA
Martin E. Strones	DoE
Jim Sullivan	CIA
Annette B. Swider	CIA
Larry D. Wilcher	DoE

Secretarial and Clerical ***Support:***

Barbara Dever	CIA
Josephine Harrison	CIA
Betty L. Richman	CIA

Table of Contents

Chapter 1.

Approaching the Next Century

As the twentieth centu y nears its end, events require that the United States assess the basic assumptions and goals that guide the protection of government information, facilities, and people.

The first duty of government is to provide security for its citizens. This security takes many forms, including a strong military, a robust economy, and mutually beneficial international relationships. In a democracy, the people's security also depends on the health of the democracy itself. This, in turn, depends on the protection of democracy's processes and the careful maintenance of the balance between the right of the public to know and the government's responsibility to provide for security.

As the twentieth century nears its end, events require that the United States assess the basic assumptions and goals that guide the protection of government information, facilities, and people. Our preoccupation with the specter of nuclear annihilation has been reduced; the resources for national security programs are declining sharply; and the information age has irrevocably altered the way we do business. Concurrently, the continued preeminent role of the United States in world political, military, and economic affairs makes our government and industrial activities of major interest to foreign powers. In this environment, the security practices and procedures that developed from World War II until the 1990s require fundamental reexamination.

For some time, it has been recognized that the security system is fragmented, complex, and costly. The Infrastructure Report of the Community Management Review requested by then Director of Central Intelligence (DCI) Robert Gates labeled current security policies and practices as the "greatest deterrents to major savings in infrastructure," and recommended the creation of a DCI security commission to design and implement a new security system. The DCI's Task Force on Standards of Classification and Control Report, commonly known as the "Gries Report," called for revision of the classification and control system on the grounds that it was "unsuited to the geopolitical and fiscal realities.. . in the 1990s." The Gulf War reinforced the military's need to analyze and move vast amounts of information to distant theaters of operation. Industry has been concerned about the inconsistency and cost of current security practices and procedures. Congress is convinced that change is necessary.

The Secretary of Defense and the Director of Central Intelligence acknowledged these concerns and established the Joint Security Commission in May 1993. The Commission's task was to review security policies and procedures with three simple goals: (1) find what works and keep it; (2) determine what no longer works and fix it; and (3) identify what the future demands and implement it.

In the nine months since its creation, the Joint Security Commission has attempted to fulfill this task by conducting an extensive security review

within the Department of Defense and the Intelligence Community In doing so, the Commission sought not only the perspectives of policymakers, the Congress, industrial leaders, the military, and public interest groups but also the technical expertise of government and industry security personnel. Many will recognize their words and opinions in the text of this report and we acknowledge a debt of gratitude for their contributions. We also commend the many initiatives already underway--such as those instituted by the National Industrial Security Program and the DCI's Security Forum-to streamline and modernize the government's security policies and practices and to incorporate risk management strategies.

The Commission's considered opinion, however, is that these changes alone are not enough. The security system must not only overcome the inefficiencies of the past but also rise to the challenges of the future. It must be dynamic, flexible, and forward looking.

Nowhere is this more apparent than in the area of information systems and networks. The Commission considers the security of information systems and networks to be the major security challenge of this decade and possibly the next century and believes that there is insufficient awareness of the grave risks we face in this arena. The nation's increased dependence upon the reliable performance of the massive information systems and networks that control the basic functions of our infrastructure carries with it an increased security risk Never has information been more accessible or more vulnerable. This vulnerability applies not only to government information but also to the information held by private citizens and institutions. We have neither come to grips with the enormity of the problem nor devoted the resources necessary to understand fully, much less rise to, the challenge. Fundamental and very tough questions are involved: What should the government's role be in help ing to protect information assets and intellectual capital that are in private hands? How should technology developed by the government to protect classified information be provided to the private sector for the protection of sensitive but unclassified information? Protecting the confidentiality, integrity, and availability of the nation's information systems and information assets-both public and private— must be among our highest national priorities.

The Commission believes that there are fundamental wealmesses in the security structure and culture that must be fixed. Security policy formulation is fragmented. Multiple groups with differing interests and authorities work independently of one another and with insufficient horizontal integration. Efforts are duplicated and coordination is arduous and slow. Each department or agency produces its own implementation rules that can introduce subtle changes or additions to the overall policy. There is no effective mechanism to ensure commonality.

The Commission believes that the complexity and cost of current security practices and procedures are symptoms of the underlying fragmentation and cannot be alleviated without addressing it. We, therefore, propose that a security executive committee be created to assume responsibility for the develop ment and oversight of security policy for the US Government and to function as a continuing agent of change. We further propose that a security advisory board be constituted to interject a nongovernment and public interest perspective into government security policy. These proposals are described in detail in chapter 11.

The Commission believes that the complexity and cost of current security practices and procedures are symptoms of the underlying fragmentation and cannot be alleviated without addressing it.

The problems are many and the mandate for change is strong, but change must be guided by clear goals and principles.

Some other problems that we identify and discuss in this report are:

- Countermeasures are frequently out of balance with the threat. They have too often been based on worst-case scenarios rather than realistic assessments of threats and vulnerabilities.

- The classification system is cumbersome and classifies too much for too long. The zeal to protect information has sometimes inhibited the flow of information to those who need it.

- Personnel security is the centerpiece of the Federal security system, but current procedures are needlessly complex and costly. There are too many inconsistencies, too many forms, and too much delay.

- There are too many layers of physical security and they cost too much money A facility's security may include multiple layers-fences, alarms, guards, security containers, access control devices, closed circuit television, locks, and special construction requirements-that are not necessarily needed.

- Large sums have been spent on technical security within the United States despite a minimal level of threat.

- Procedural security measures are not always effective. Elaborate recordkeeping procedures for document control are costly and can no longer be relied upon to deter compromise in the age of personal computers, facsimile machines, copier equipment, modems, and networks which offer ample opportunities to copy documents without detection. Procedural security that is still necessary, such as badges and visitor control, can be streamlined.

- Operations security (OPSEC) is important and sometimes critical in a military environment and for sensitive operations, but it has been extended to inappropriate situations and environments.

The problems are many and the mandate for change is strong but change must be guided by clear goals and principles. We envision security as a dynamic and flexible system guided by four basic principles:

- Our security policies and services must be realistically matched to the threats we face. The processes we use to formulate policies and deliver services must be sufficiently flexible to facilitate their evolution as the threat changes.

- Our security policies and practices must be consistent and coherent across the Defense and Intelligence Communities, thereby reducing inefficiencies and enabling us to allocate scarce resources efficiently.

- Our security standards and procedures must result in the fair and equitable treatment of the members of our communities upon whom we rely to guard the nation's security.

- Our security policies, practices, and procedures must provide the security we need at a price we can afford.

The Commission believes that the application of these principles will make the security system less fragmented, less complex, and more cost effec-

tive. We also believe that the progress made will be eroded over time without a fundamental adjustment in the way security is viewed and practiced. Security can no longer be seen as an independent, external authority that rigidly imposes procedures and demands compliance. The Commission believes that it is time for a paradigm shift.

- Security is a service that should be based on an integrated assessment of threat, vulnerability and customer needs. Conceptually, it should be the way that we think rather than a manual of rules. Security then becomes a more positive undertaking that values the spirit over the letter of the law, problem prevention over problem resolution, and individual responsibility over external oversight. It is a partnership between security and operations that balances the need to protect with the need to get the job done. Industry is a valuable partner and participant in this process.

- Security must come from an integrated system that recognizes the interdependence of the individual security disciplines and establishes a logical nexus between the sensitivity of information and the personnel, physical, information, and technical security countermeasures applied in protecting the information. In this model, the individual security disciplines are interlocking pieces of a puzzle, each critical to overall success but none sufficient by itself.

- Security is a shared responsibility Each individual has a role to play in ensuring the best possible protection for our information, personnel, and assets. Individual and management accountability for security actions and decisions are prerequisites for dynamic and responsive security processes.

- Security is a balance between opposing equities. The imperative to protect cannot automatically be allowed to outweigh mission requirements or the public's fundamental right-to-know and it must never obscure the understanding that an informed public is the foundation of a democratic government.

Implementing the New Paradigm-Risk Management

In the past, most security decisions have been linked one way or another to assumptions about threats. These assumptions frequently postulated an all-knowing, highly competent enemy. For the better part of the last half century, we viewed the Soviet Union and its allies as capable of exploiting our every weakness. Against this danger, we strove to avoid security risks by maximizing our defenses and minimizing our vulnerabilities. Since the future of the free world was considered highly dependent on how successfully we maintained our secrets, the costs of security programs, the constraints on needed information flow, and the negative impact on individuals and our economic competitiveness were all secondary considerations. We used worst case scenarios as the basis for most of our security planning.

The threats today are more diffuse, multifaceted, and dynamic. National security concerns now include a daunting array of challenges that continue to grow in diversity in our unstable and unpredictable world. The possibility of failure of democratic reform in Russia poses a constant danger. Further, Russia's ability to maintain control of its special weapons, China's supplying of equipment and technology to unstable countries, and North Korea's, Iran's and Iraq's attempts to develop nuclear weapons, have serious and far-reach-

The threats today are more diffuse, multifaceted, and dynamic. National security concerns now include a daunting array of challenges that continue to grow in diversity in our unstable and unpredictable world.

ing implications for regional security and stability. Burgeoning ethnic and religious rivalries that cross traditional boundaries endanger both *new* and long-standing peace agreements, drawing the United States into an expanding role in peacekeeping and humanitarian missions. The bombing of the World Trade Center and the assassination of two CIA employees in Via heightened our sensitivity to the fact that terrorist activities against Americans can occur domestically as well as abroad. Violent crime and narcotics trafficking in our neighborhoods also continue to threaten American lives and values.

We can and must provide a rational, cost-effective, and enduring framework using risk management as the underlying basis for security decisionmaking.

The Commission recognizes that the consequences of failures to protect against some of these threats are exceptionally dire. For instance, terrorists' use of weapons of mass destruction, or an adversary's foreknowledge of our battle plans, could have consequences so grave as to demand the highest reasonably attainable standard of security. This is true even if the probability of a successful attack is small and the cost of protection is high. Some inherent vulnerabilities can never be eliminated fully, nor would the cost and benefit warrant this risk avoidance approach. In most cases, however, it is possible to balance the risk of loss or damage of disclosure against the costs of countermeasures and select a mix that provides adequate protection without excessive cost in dollars or in the efficient flow of information to those who require ready access to it. We can and must provide a rational, cost-effective, and enduring framework using risk management as the underlying basis for security decisionmaking.

The Commission views the risk management process as a five-step procedure:

1. Asset valuation and judgment about consequence of loss. We determine what is to be protected and appraise its value. Part of asset valuation is understanding that assets may have a value to an adversary that is different from their value to us.

2. Identification and characterization of *the* threats *to specific* assets. Intelligence assessments must address threats to the asset in as much detail as possible, based on the needs of the customer. These assessments may be. commissioned at the national level to feed the development of security policies and standards, at the program level to guide systems design, or in planning intelligence support for military or other operations.

3. Identification and characterization of the vulnerability of specific assets. Vulnerability assessments help us identify weaknesses in the asset that could be exploited. The manager may then be able to make design or operational changes to reduce risk levels by altering the nature of the asset itself. Cost is an important factor in these decisions, as design changes can be expensive and can impact other mission areas.

4. Identification of countermeasures, costs, and tradeoffs. There may be a number of different countermeasures available to protect an asset, each with varying costs and effectiveness. In many cases, there is a point beyond which adding countermeasures will raise costs without appreciably enhancing the protection afforded.

5. *Risk assessment.* Asset valuation, threat analysis, and vulnerability assessments are considered, along with the acceptable level of risk and any uncertainties, to decide how great is the risk and what countermeasures to apply.

This process is depicted in the following figure:

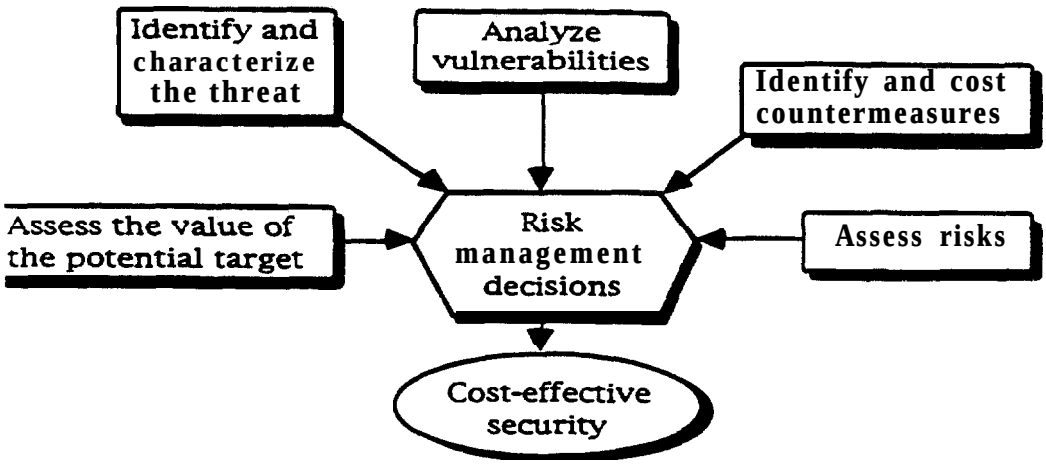


Figure 1. The Risk Management Process

When any of these steps are left out, the result can either be inadequate protection or unnecessary and overly expensive protection. Frequently, the missing element is the incorporation of specific, **up-to-date** threat assessments in the development of security policies. With no documented threat information, countermeasures are often based on worst case scenarios.

The Commission stresses that managers must make tradeoffs during the decision phase between cost and risk, balancing the cost in dollars, manpower, and decreased flow of needed information against possible asset compromise or loss. Policy decisions resulting from the risk management process can then guide security planning. At the national level, these risk management decisions should form the backbone of, and provide the standards for, the security system. The resulting **standards** would promote consistency, coherence, and reciprocity across programs and agencies.

Managers must make tradeoffs during the decision phase between cost and risk, balancing the cost in dollars, manpower, and decreased flow of needed information against possible asset compromise or loss.

Chapter 2.

Classification Management

[Classification] deals with only a small slice of the government information that requires protection although ii drives the governmen t's security apparatus and most of its costs.

Classification-Driving Security

The classification system is designed primarily to protect the confidentiality of certain military, foreign policy, and intelligence information. It deals with only a small slice of the government information that requires protection although it drives the government's security apparatus and most of its costs.

Despite the best of intentions, the classification system, largely unchanged since the Eisenhower administration, has grown out of control. More information is being classified and for extended periods of time. Security rules proliferate, becoming more complex yet remaining unrelated to the threat. Security costs increase as inconsistent requirements are imposed by different agencies or by different program managers within the same agency.

This accretion of security rules and requirements to protect classified information does not make the system work better. Indeed, the classification system is not trusted on the inside any more than it is trusted on the outside. Insiders do not trust it to protect information that needs protection. Outsiders do not trust it to release information that does not need protection.

This Cold War classification system can be simplified. In place of more than 12 levels of protection and widely differing and inconsistent security policies and practices, the Commission recommends a single, rational, governmentwide standard for the protection of classified information.

The Current Classification System—Cumbersome and Confusing

The classification system is more complex than necessary. Classification is inherently subjective and the current system inappropriately links levels of classification with levels of protection.

The current classification system starts with three levels of classification (Confidential, Secret, and Top Secret), often referred to collectively as collateral. Layered on top of these three levels are at least nine additional protection categories, These include Department of Defense Special Access Programs (DoD SAPs), Department of Energy Special Access Programs, Director of Central Intelligence Sensitive Compartmented Information Programs (DCI SCI), and other material controlled by special access or 'bigot" lists' such as the war plans of the Joint Chiefs of Staff and the operational files and source information of the CIA Operations Directorate. Further complicating the system are restrictive markings and dissemination controls such as ORCON (dis-

semination and extraction of information controlled by originator), NOFORN (not releasable to foreign nationals), and "Eyes Only."

Classification	Levels of Protection		
TOP SECRET	TS-BIGOTLIST	TS - SCI	TS - DoD SAP
SECRET	S -BIGOTLIST	S - SCI	S - DoD SAP
CONFIDENTIAL	C - BIGOT LIST	C - SCI	C -DoDSAP
UNCLASSIFIED			

Figure 2. The Current Classification System

Currently, proper classification depends on assessing the expected damage to national security caused by unauthorized disclosure of the information. Information is classified as Confidential if damage is expected to occur. Secret is used if serious damage will result. Information is Top Secret only if exceptionally grave damage will occur. However, because it is difficult to precisely define levels of damage, reasonable persons can and do differ in their evaluation. Yet, it is not even clear why the effort to assess damage should be made since the protection required is not dependent on the level of damage. For example, greater protection is provided for Secret information in SCI channels, disclosure of which would cause "serious damage" to national security, than for Top Secret information that is not within a special access program, disclosure of which would cause "exceptionally grave damage." Moreover, from a Freedom of Information Act or an Espionage Act standpoint, the significant issue is whether the information is classified, not the level at which it is classified.

We conclude that there is no need for levels of classification. Information is not more classified or less classified. It either is classified or it is not. Indeed, thinking about information as more or less classified has led to statements that information is "only Confidential" or "only Secret." This thinking also has led to efforts to link classification levels with the length of time protection is required. Yet we know that some Top Secret information, such as an invasion date, may need to be protected for days, while some Secret information, like the identity of a confidential source, may need to be protected for decades.

There is no need for levels of classification. Information is not more classified or less classified.

Special Access Programs-Lacking Faith in the System

Special access programs[2] are used to compensate for the fact that the classification system is not trusted to protect information effectively and does not adequately enforce the "need to know" principle. For example, the Top Secret classification is supposed to protect information that, if improperly disclosed, would result in exceptionally grave damage to the national security. Yet, the perception is that the "regular" classification system cannot protect such information because it has no provision for limiting which cleared persons have access to the information.

In the 1980s, as confidence in the traditional classification system declined, more and more information was put into SAP and SCI compart-

As confidence in the traditional classijcation system declined, more and more information was put into SAP and SCI compartments.

ments based on assertions that the regular classification system provided inadequate need-t&now restrictions. The special access system gave the program manager the ability to decide who had a need-to-know and thus to strictly control access to the information. But elaborate, costly, and largely separate structures emerged. According to some, the system has grown out of control with each SAP program manager able to set independent security rules.

The Department of Defense divides these programs into three categories: acquisition, intelligence, and operations and support.[3] Programs in these cat& gories are further defined as either acknowledged or unacknowledged! Some of the most sensitive DoD programs are "waived" or "carved out" from certain oversight and administrative requirements. There are over one hundred DoD SAPs, with many having numerous compartments and subcompartments, designed to further segregate and limit access to information. Each special access program manager is free to establish the security rules that will apply to his or her particular program.

Within the Intelligence Community, the term Sensitive Compartmented Information (SCI) refers to data about sophisticated technical collection systems, information collected by those systems, and information concerning or derived from particularly sensitive methods or analytical processes. Specific SCI control systems serve as umbrellas for protecting a type of collection effort or a type of information. Within each SCI system are compartments and within them, subcompartments, all designed to formally segregate data and restrict access to it to those with a need-to-know, as determined by a central authority for each system. There are over 300 SCI compartments (recently reduced from over 800) grouped into a dozen or so control channels. Special activities have their own non-SCI control channels. Rules relating to SCI programs are found in DCI Directives (DCIDs), but implementation is uneven and minimum standards are often exceeded.

In addition to the formal SAP, SCI, and covert action control channels, strict need-to-know access restrictions also are imposed for other types of information within the DoD and the Intelligence Community. These include information identifying intelligence sources and liaison relationships, as well as information about military plans, such as the Single Integrated Operations Plan (SIOP) for strategic nuclear war or the battle plan for the invasion of Iraq during the Gulf War. Access to such information is generally controlled by access or bigot lists.

The Commission agrees that some types of classified information, such as identities of intelligence sources, information about sensitive intelligence methods, plans for operations, and technological advances that provide our military forces unique advantages on the battlefield, may require more protection than others. However, we do not agree that each SAP manager needs to establish a unique set of security rules, or that SAP security rules and SCI security rules need to be different. Current practice has begun to recognize this fact and to coalesce around two standards: one for Confidential and Secret, the other for Top Secret and SAPs/SCI. In personnel security, for example, agencies do not have separate clearance standards for Confidential and Secret. And a single clearance standard for Top Secret and SCI is evolving with DoD SAPs beginning to follow this standard, even though program managers today have the authority to impose their own standards and many do so.

A New System-Streamlined and Straightforward

The opportunity to change the classification system comes at an important point in our history. In this post-Cold War period, we can move away from a strategy that has been characterized as something close to total risk avoidance and develop instead an approach more clearly based on risk management. We continue to recognize that there is information that needs the protection of the classification system and that there are costs associated with the unauthorized disclosure of information vital to the national security. But we also recognize that in a democracy the public needs access to information about what its government is doing and that there are significant costs associated with keeping information classified and tightly controlled. In sum, it is important to consider the political, economic, and opportunity costs of classifying information, as well as the costs of failing to classify **information.**

It is important to consider both the political, economic, and opportunity costs of classifying information as well as the costs of failing to classify information.

The Commission finds that the costly and complicated bureaucracy that provides security is a reflection of the underlying complexity of the classification management system. The Commission believes that a less complicated system can help correct the current approach that has led to classifying too much at too high a level and for too long. We propose **a** new one-level classification system. Under this system, information either is classified or it is not. There would be a single legal definition of classified information and no need to pretend that we can precisely measure the amount of damage to national security that would be caused by an unauthorized disclosure.

Two degrees of protection will be available, instead of the dozen or so now used. Information either will be generally protected (labeled SECRET) or specially protected (labeled SECRET COMPARTMENTED ACCESS). Each protection level would be defined both in terms of the type of information to be included and the type of protection. The protections available for each level will be standardized. Most special handling and dissemination markings will be unnecessary and special access controls will be integral to, rather than added onto, the classification system. In addition, only certain clearly defined categories of information will qualify for special protection and only in certain clearly defined circumstances.

Classification	Levels of Protection
Classified	SECRET
	SECRET CONTROLLED ACCESS
Unclassified	

Figure 3. The Proposed Classification System

The vast majority of classified information would be generally protected to promote the availability and accessibility of the information. Baseline security protection standards will be established and discretionary need-to-know would apply; a cleared individual could determine whether to pass the information to another cleared individual. Generally protected information would incorporate current Confidential and Secret documents, which will not have to be remarked.

The Commission recognizes that most departments and agencies have, and will want to continue, procedures that govern the manner in which Secret

information is disseminated within their organizations. Some may also wish to maintain limited control on their information that is passed to other agencies, such as a requirement that the recipient agency not pass the information on to a third agency without obtaining permission from the originating agency. Finally, there may be unique problems that arise in implementing this new approach that require an exemption from general rules, such as the manner in which CINCs communicate with Navy vessels. The Commission recognizes the need for flexibility, but does not want to lose the advantages of the new system through creating loopholes by, for example, permitting heads of departments and agencies to create "mini SAPs" by imposing dissemination controls. Therefore, the Commission recommends that heads of departments or agencies be permitted to establish dissemination controls on Secret information only upon approval of the security executive committee proposed in chapter 11.

As a result of risk analysis, a limited amount of information would be specially protected as Secret Compartmented Access information. Enhanced security protection standards would apply, requiring a higher clearance standard for access and a centralized need-to-know control structure provided by an access or bigot list. Compartmented access information would incorporate most current Top Secret, Special Access, and Sensitive Compartmented Information.

The Commission fmds that classification management is the "operating system" of the security world. Classification drives the way much of security policies are implemented and security practices are carried out. Standards, organizations, procedures, and policies governing everything from the levels of security clearance, to procedures for processing information, to sentencing guidelines for individuals convicted of espionage are based on our existing classification structure. The complexity of the existing classification system is the root cause for much of the confusion of the existing security system.[5] Simplify the classification system and simplification of the security system will follow.

Simplify the classification system and simplification of the security system *will follow.*

The Commission notes that the existing classification management system is evolving naturally into a two-level system. Confidential and Secret information is handled using similar or identical standards. Top Secret, SCI, and SAP information is protected using more stringent and substantially common standards. The Commission believes that this natural occuring division forms an excellent basis for an improved classification system.

The proposed system will better relate needed asset protection to security countermeasures. In place of the myriad investigative and adjudicative requirements and the differing physical security standards, two security standards, based on analysis of risk, would be developed to guide application of the two degrees of protection for these security disciplines. Procedures for securing classified information would likewise have only two standards. Similar simplifications would follow throughout the rest of the security system.

The Commission recommends **the establishment of a one-level classification system with two degrees of protection.**

A Simplified Controlled Access System

The Commission concludes that the current special access system needs to be simplified. Enhanced security protection can be achieved with less compartmentation and fewer barriers to the flow of information. Instead of the current complicated system with the multiple control officers and multiple control channels, information requiring special protection would be marked SECRET COMPARTMENTED ACCESS and would carry a designator, such as a codeword or number, identifying the relevant access list. A single specially protected information control officer and channel would replace the panoply of structures and systems for protecting SCI, SAPs, or bigot list controlled access information.

Thus, instead of the structure shown below in figure 4:

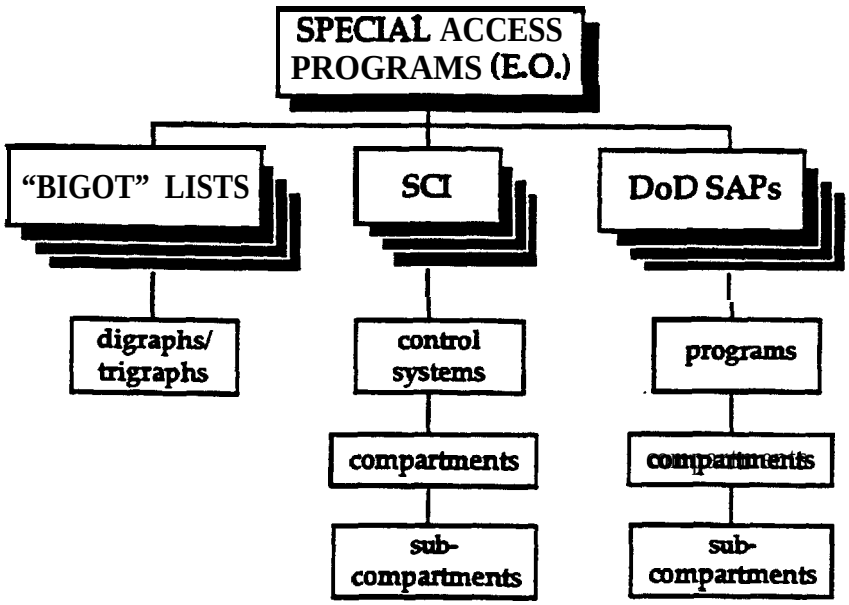


Figure 4. ***Current Special Access Programs Structure***

We propose the following structure:

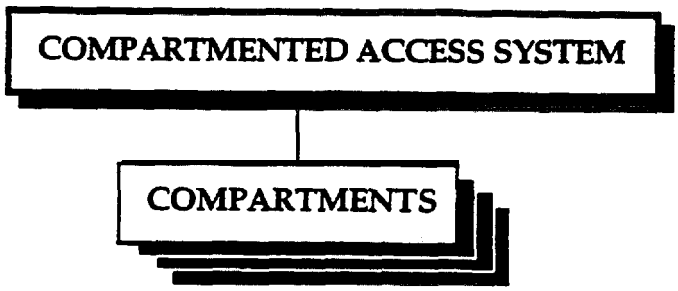


Figure 5. Proposed Sped ***Access Programs Structure***

The Commission recommends that:

a) All special access, SCI, covert action control systems, war plans and bigot list activities be integrated into the new classification system.

b) A single control channel for SECRET COMPARTMENTED ACCESS information, with a codeword for each need-to-know list, replace all existing special control channels.

Steps will be taken to limit the amount of information that is specially protected and to prevent the migration of information from the generally protected level to the specially protected level.

Limiting Use of Special Access Controls

The Commission concludes that simplifying the system will aid in identifying and better protecting information that really needs enhanced security protection. Viewing information as part of a special access program often meant that everything in the program had to be compartmented. Analyzing the impact of the loss of specific information focuses attention on what needs special protection and what does not, and would result in less information being placed at the compartmented access level.

Steps will be taken to limit the amount of information that is specially protected and to prevent the migration of information from the generally protected level to the specially protected level. A first step is to identify clearly in an executive order those limited categories of information qualifying for special protection.

The Commission suggests the following categories of information be considered for special protection:

- A technology application that provides a significant battlefield edge and that could be copied or countered if key information were disclosed to a potential adversary.
- A sensitive military operation or plans for the operation in circumstances in which disclosure might impair its current or future success.
- A fragile intelligence method when the opposition is not aware of either the fact, or special capabilities of the method and, were they to become aware of it, could employ countermeasures to deny us information or use deception to feed the US incorrect information.
- A human source in circumstances in which the US would lose its ability to use the source and/or the source or the source's family is likely to be harmed.
- A sensitive intelligence, counterintelligence, or special activity in circumstances in which disclosure would impair its success.
- Information that would impair US cryptologic systems or activities.

- **Sensitive policy issues** or **relationships with a foreign government** which, if revealed, would significantly harm foreign government cooperation with the US.

- A **US negotiating position** in circumstances in which such disclosure would cause us to lose a negotiating advantage.

- Scientific and technical information that describes the design of **weapons of mass destruction** that could significantly assist others to develop or to improve such weapons, or to significantly enhance their ability to circumvent the control features of such weapons.

The Commission recommends that compartmented access be considered for the categories of information detailed above and any other categories of equally sensitive information, and that all current and future Special Access Programs, war plans requiring limited access controls, Sensitive Compartmented Information, covert action control systems, and bigot lists be reviewed and validated against that list.

Critical specially protected information within the various DoD and SCI compartments is not clearly identified.

Perhaps the greatest weakness in the entire system is that critical specially protected information within the various DoD and SCI compartments is not clearly identified. Individuals within government and industry are forced to protect everything within a particular compartment, rather than just the small amount of information that truly needs compartmented access status and need-to-know controls.

> *One general officer likened the situation to trying to protect every blade of grass on a baseball field. He had to have a hundred players to guard the entire field, when only four persons to protect home plate would suffice.*

The Commission believes a rigorous review is needed to identify and separate the information that will continue to require special protection from that which does not. Such a review will allow many compartmented access compartments to be eliminated and will permit the consolidation of critical data within fewer remaining compartments.

The Commission recommends that the Secretary of Defense and **the Director of Central Intelligence direct that managers for each compartmented access system undertake a review to identify information within all compartments and subcompartments that requires continued special protection. This information should be consolidated** in **the fewest compartments possible.**

Uniform Risk Criteria for Secret Compartmented Access Information

The Commission believes that decisions to require special protection for sensitive information and activities should be consistently made based on common risk management principles.

Uniform risk assessment criteria do not exist for establishing, designating, managing, and disestablishing SAP and SCI compartments.

The Commission found that uniform risk assessment criteria do not exist for establishing, designating, managing, and disestablishing SAP and SCI compartments. Each component develops its own procedures for assessing the risks dictating compartmented access protection, often with little external guidance or oversight. Some elements place unclassified technologies and independent research and development efforts directly under special protection as soon as a promising military application is discovered. Others do not, and thus disparities exist among agencies in the way the same basic technology or application is classified, designated, and protected.

The decision to designate a DoD SAP as unacknowledged radically increases its cost and severely inhibits oversight, coordination, and integration with other similar programs. Critics advised the Commission that state of the art advances and efficiency gains may be sacrificed or significantly hindered once a technology-based program is brought under special controls. If an acquisition SAP is unacknowledged, others working in the same technology area may be unaware that another agency is developing a program. The government may pay several times over for the same technology or application developed under different special programs within different agencies.

> *Two military services and the DoE have programs involving the same technological application. One militia y service classified its program as Top Secret Special Access with a deadlyforce protection requirement. The other* military service *classified* its program *as Secret Special Access* with *little more than tight need-to-know protection applied. The DoE classified its program as collateral Secret, adopting discretionary need-to-know procedures.*

Despite the fact that the Commission did find one or two examples of programs coordinating common technology or scientific issues, the potential still exists for disconnects in coordination and integration among various DoD SAPs and non-SAP programs. In the above example, the three government agency program managers are aware of the other programs, but refuse to devise a common protection standard. This problem is not uncommon. The strict SAP control inhibits the flow of information. One result is that comparable advances in state-of-the-art technology by related noncompartmented government research efforts are not readily accepted by some SAP managers as valid reasons to decompartment their programs. The government pays a high cost when this occurs. Continuing special security controls when they may not be necessary is expensive. But, the controls are probably much less costly than the lost opportunities caused by inhibiting non-governmental research initiatives with potential payoffs for the SAP itself.

The Commission applauds the DoD's action to establish joint coordination and review of Stealth and related low-observable technologies developed by numerous special programs. However, this effort should be expanded to achieve integration across the DoD components and non-DoD agencies in other areas of technology to reduce apparent gaps in the integration of SAP

decisions with national-level science and technology intelligence, counterintelligence, and counterproliferation intelligence analysis. Again, using the example above, a common security standard is needed to reduce conflicting analyses regarding the true state-of-the-art or the actual threat to advanced technologies that in turn leads to the application of varying degrees of security and the resulting costs.

There also is the need for coordination of DoD special program issues and decisions with other governmental interests, such as foreign relations with the Department of State and national intelligence issues with the Director of Central Intelligence. In the past, decisions were made not to brief the Director of Central Intelligence on certain DoD programs that affected national intelligence interests. Such decisions can occur when senior-level personnel are not made aware of, for example, the existence of a subcompartment or the impact of certain activities under special programs.

The Commission's recommendations on threat assessment and risk management should be followed in determining whether and how special protection is to be applied, especially with respect to unacknowledged programs. This criteria should form the basis for decisions made on special protection throughout the government.

The Commission recommends that the Secretary of Defense and the Director of Central Intelligence:

a) Establish uniform risk assessment criteria for the consideration, designation, review, management and decompartmentation of information requiring special protection,

b) Conduct independent risk assessments of the unacknowledged status of compartmented access programs, based upon all-source analysis of relevant intelligence and counterintelligence information.

c) Review similar compartmented access programs to ensure reciprocity and eliminate redundancy.

d) Institute a formal mechanism to review designation, coordination, and integration issues related to compartmented access programs to ensure that the DoD elements, the Intelligence Community, the Departments of State, Energy, Commerce, and others are advised of compartmented access program issues affecting their interests.

Currently, SAP security policies are developed independently by individual program managers. Within the Intelligence Community, actual SCI program practices often exceed the DCID standard. The Commission found that many of the problems with the SAPs and the SCI programs are due to obsolete security standards and inconsistent, program-specific applications. The conflicting policies of the DoD and Intelligence Community elements add significant unnecessary expense to the system, with no appreciable increase in security. Common standards for special protection would bring coherence to the DoD and Intelligence Communities, and bridge the gap between the DoDs SAPs and the DCI's SCI programs.

Under the new classification scheme, the security executive committee, described in chapter 11, will work with security professionals and program managers to develop a single uniform security policy and set of standards adequate to protect all DoD and Intelligence Community special programs. As a consequence, there no longer would be the wide variances in security practices that significantly raise costs, particularly in industry Managers of special programs would not be granted unbridled discretion in deciding which security measures to employ, but they would be allowed to waive down from the standard in circumstances in which reciprocity is not affected: In sum, reciprocity, integration, and the ability to control overall costs requires that a uniform standard be followed in most cases, but exceptions could be made in appropriate circumstances.

Reciprocity, integration, and the ability to control overall costs requires that a uniform standard be followed in most cases.

The Commission recommends that:

a) A single, consolidated policy and set of security standards be established for Secret Compartmented Access information, including all current SAPs, SCI, covert action, and the various bigot list programs.

b) Standards contain some flexibility, but waivers down from compartmented access security measures be permitted only **when there is no impact upon reciprocity.**

Increasing the Flow of Data

Many persons who spoke to the Commission were quite critical of the Intelligence Community's tendency to disseminate intelligence data within compartmented channels rather than at the generally protected level. Combatant commanders are adamant that intelligence must be released at the Secret level to be useful to them. Law enforcement agencies increasingly assert that most intelligence information passed to them is overclassified and therefore often unusable. Excessive compartmentation precludes the timely dissemination of intelligence pending completion of reviews to remove (or sanitize) source and method revealing information or until permission is granted for release of originator-controlled **data.** This has an adverse impact on the timeliness and specificity of intelligence. The impact is very serious to users of intelligence in the DoD, its agencies, and the military services.

> *During the Gulf War,* the *limited amount of sanitized operations-related intelligence information forced one military officer to meet his warfighting needs by regularly flying two Captains back and forth to US installations in Europe* to *get additional information decompartmented and then* to *return with as much of this hard copy intelligence data and imagery as they could carry.*

All users made clear to the Commission that they want intelligence provided in a more timely manner, with **as** much specificity as possible, and with fewer dissemination restrictions. Currently compartmented data should be reviewed to remove source- or method-revealing information so that significantly more intelligence information can be made available as generally protected information. Those sanitizing intelligence should also ensure as much

usable data remains as possible. Concerns have been raised that, at times, so much information is removed in order to protect sources and methods, the ability of users of the information to make critical decisions is undermined.

The Commission is encouraged by efforts under way to limit the amount of controlled access information within the Intelligence Community. Most intelligence reporting based on human sources is not compartmented because source-identifying information is deleted. Further, a significant amount of imagery is being released outside of compartmented channels. While the National Security Agency has made progress in decompartmenting its information, more can be done. Significant benefit would be gained if the National Security Agency were to form a task force, similar to the one formed by the Central Imagery Office, to drastically reduce the amount of compartmented information it produces, and to release more intelligence at the generally protected level.

The Commission believes that, as a general rule, only the limited amount of intelligence that would materially compromise sensitive sources and methods or collection strategies, as well as that which has exceptional political sensitivity due to the nature of the target, should remain within compartmented channels. The remaining vast majority of data should be routinely released as generally protected information. Where source-revealing information must necessarily be included, the Commission strongly recommends the use of a tear line. Those who need to know how the information was derived will have access to the information above the tear line, marked SECRET COMPARTMENTED ACCESS. Those who need to act on the information, but do not need to know the source of the information, will receive the generally protected information below the tear line, marked SECRET.

The Commission recommends that:

a) All intelligence reporting within compartmented channels be severely restricted to the limited amount of information that would coinpromise sensitive sources and methods or collection strategies, or that has exceptional political sensitivity.

b) All other intelligence products, particularly when related to military operations, be released as generally protected information.

Advanced weapon systems and specialized intelligence capabilities are of little use to the military commander if he is unaware of them and unable to train warfighting elements in the use of the new capability. Briefing commanders when compartmented **access** programs are ready for use is not enough. Military elements must be kept aware of the program, its goals and objectives, and its potential employment well ahead of production and deployment in order to fully incorporate new capabilities into unit war plans.

Although many technologies, weapon systems, and intelligence capabilities are ultimately developed for use by the warfighter, no effective procedure exists to ensure that combatant commanders are briefed on all such systems, their capabilities, and projected availability for use. Moreover, the Commission found that even when military elements are briefed, they are put under such tight constraints that they are unable to use the compartmented access information in any practical **way.** This prohibits field elements from being

All users . . . want intelligence *provided in a more timely manner, with as much specificity as possible, and with fewer dissemination restrictions.*

able to incorporate these capabilities into war planning and *other* crisis activities.

> *A senior military officer on fhe Joint Staff expressed concern fhat current classification and security procedures constrict the flow of operational information to the warfighter at the tactical level. He felt that we still treat certain capabilities as pearls foo precious fo wear-we acknowledge their value, but because of their value, we lock them up and don't use fhem for fear of losing them.*

More *needs to be done to keep combatant commanders informed of current and upcoming programs, capabilities, weapons, or operations that could potentially be used in a military scenario.*

The Commission believes that more needs to be done to keep combatant commanders informed of current and upcoming programs, capabilities, weapons, and operations that could potentially be used in a military venue. Accordingly, a separate, small entity should be established and given the responsibility to work with the owners of compartmented **access** information to disseminate it aggressively to combatant commanders. This entity, with full access to all compartmented access programs, would balance the perceived reluctance of special access program managers to share **information** against the perceived tendency of military entities to disseminate this information broadly within a command. The intent is to ensure that combatant commanders are more fully informed about compartmented access activities while taking into account the sensitivity and fragility of the information.

The Commission recommends that the Secretary of Defense and the Director of Central Intelligence:

a) Establish a separate entity to work with special access program managers and combatant commanders to ensure that military commands are more fully aware of compartmented access information concerning current and projected technologies, weapons, techniques, operations and programs that are pertinent to their responsibilities.

b) Delegate authority to combatant commanders to brief staff members with a need-to-know on compartmented access information so that these capabilities can be incorporated into conflict planning activities.

Special Cover Measures

There are many valid reasons for the special cover measures used by some military and intelligence organizations, such as potentially life-threatening, high-risk, covert operations and intelligence and counterintelligence investigations or operations. However, these techniques also have increasingly been used for major acquisition and technology-based contracts to conceal the fact of the existence of a facility or activity or to mask government-contractor affiliations.

The Commission found that the use of cover to conceal the existence of a government facility or the fact of government research and development interest in a particular technology is broader than necessary and significantly increases costs. For example, one military service routinely uses cover mechanisms for its acquisition controlled access programs without regard to indi-

vidual threat or need. Another military organization uses cover to hide the existence of certain activities or facilities. Critics maintain that in many cases, cover is being used to hide what is already known and widely reported in the news media.

> *Several government agencies paid, under various secure contracts, to have a significant number of "sterile" telephones installed to hide contractors' affiliations with the government. In many cases, the sterile telephones were installed next to secure telephones required by other classified government* contracts. *in one case, a contractor had 200* sterile *telephones nexf* to 173 *STU-III telephones and 145 secure "green" phone lines.*

These cover mechanisms are expensive and the marginal security benefits gained by compartmenting knowledge of the existence of a government or contractor facility often are outweighed by the costs of concealment, including the costs to other programs that would benefit from sharing technical knowledge and sharing use of the facility. Special protection generally should focus on the most sensitive uses of a facility, rather than the fact of its existence.

Organizations with high-funding profiles and extensive contracts, such as the National Reconnaissance Office, have incorporated elaborate rules into their daily operations to conceal the fact of their existence and to hide the identity and affiliation of organization employees and contractors. Even though the NRO's existence was finally declassified in 1992, classification for most of its personnel and activities remains in place. We believe many NRO classification requirements currently imposed can be dropped without danger to essential NRO activities.

The Commission believes an overall review of the DoD and Intelligence Community organizations employing cover mechanisms is needed to determine whether such costly mea&& continue to be necessary.

The Commission recommends that the Secretary of Defense and the Director of Central Intelligence:

a) Rescind blanket classified status for the NRO and its employees.

b) Review the cover status of the DoD and Intelligence Community elements and personnel, rescinding cover for those without a documented covert intelligence or operational mission.

c) Review existing covert contractual requirements to determine those that may be canceled as soon as advantageous to the government.

d) Develop new policies for cover that limits its use to those situations for which it is needed.

Security Oversight of Compartmented Access Programs

The DoD management framework provides for oversight of all DoD compartmented access programs through reviews by the Deputy Secretary of Defense. Oversight is also provided by reports to Congress. The Commission has reviewed the reporting procedures that exist with respect to Congres-

sional oversight of the DoD controlled access programs, including those for programs that are waived from certain requirements due to their extreme sensitivity. We see no need to modify existing reporting procedures and believe that the current system should continue without change.

Until recently there has been no procedure for centralized assessment of special program proposals submitted directly to the Deputy Secretary of Defense by the military departments. The recent formation of the DoD Special Access Program Oversight Committee, which the Commission fully supports, will ensure that every program is reviewed by a panel of senior officials prior to its establishment, and annually thereafter, to determine whether compartmentation for each program is still required. This new management structure is an important initiative to improve centralized review, cross-program integration, security policy guidance, and oversight of special programs.

An independent viewpoint is necessa y to interject an unbiased, broader perspective on controlled access proposals and practices.

The Commission suggests that the Oversight Committee expand this review to incorporate a separate evaluation of the proposed or actual security countermeasures for each special program. A separate review could yield alternate security countermeasures to replace the sometimes costly or inefficient countermeasures proposed by the sponsoring special program managers. For existing controlled access programs, the Committee should examine how previously-approved security countermeasures are actually implemented. This may reveal security practices that are no longer necessary and help to lessen the gap between actual practice and policies for controlled access programs. Finally, the Commission believes that security cost-drivers, such as unacknowledged special program status, imposition of cover, mandatory polygraphs for access, and waivers from Defense Investigative Service inspections of contractors, should be considered and approved separately by the DoD Special Access Program Oversight Committee before they are unposed. These steps will aid the Oversight Committee in eliminating unnecessary and costly security practices and in redirecting scarce protection resources to other program priorities.

The Commission believes that the DOD'S new approach to overseeing controlled access programs is reasonable. However, the Commission believes the process could be strengthened by establishing a security oversight arm that is wholly independent from the everyday management and security of controlled access programs. An independent viewpoint is necessary to interject an unbiased, broader perspective on controlled access proposals and practices because many believe that SAPs are created not simply for security reasons, but to create a specialized cadre of experts, streamline procurement, limit oversight, and thus speed development. Others are concerned that fundamental questions about the propriety of controlled access activities may not be raised by those within the special program community, or be presented to senior policymakers outside of the sponsoring military service. This new oversight function would have to have up-front, across-the-board access to all special access programs.

The Commission's proposed independent oversight arm also would provide valuable guidance with respect to access control practices applied to programs other than recognized SAPs. In the past, certain DoD components have limited the distribution of particular types of classified information, such as military plans, without formally designating the program as a SAP, because SAPs require high-level approval and oversight. These programs use labels such as LIMDIS (limited distribution), SPECAT (special category), or other

less formal designations. The Commission views these programs as "SAP-like" in that aspects of approved specially protected programs, such as multiple compartments and nondisclosure agreements, often are imposed upon those given access to the information. However, DoD officials have taken the position that compartmentation to protect military plans should not be considered a "program" within the meaning of Special Access Program regulations, but simply a "planning document." As a result, military plans currently are not included in senior-level special program reviews.

In the future, none of these "plans versus program" distinctions should matter under the Commission's proposed new classification structure. However, independent oversight will continue to be necessary for controlled access programs to ensure that security issues are fully aired to senior management. Assigning independent responsibility for conducting inquiries regarding activities protected by special programs and similar compartments, will give the Secretary of Defense a valuable check and serve as a safety valve in ensuring that security protections are not misused, and that questionable practices are brought to light and resolved within the Department.

The day-to-day most serious problem is that we don't get intelligence to the policymakers in a way that they can use it.

The Commission recommends that the Secretary of Defense:

a) Under the auspices of the **DoD Special Access Program Oversight Committee:**

1) Conduct a separate evaluation of proposed or actual security countermeasures for controlled access programs.

2) Separately review and approve unacknowledged status, imposition of cover, mandatory polygraph for access requirements, and waivers from Defense Investigative Service security inspections of contractors before they may be imposed on controlled access programs.

b) Assign security oversight responsibilities for controlled access activities to an independent DoD office outside the special program community.

CLASSIFICATION MANAGEMENT PRACTICES

There are a number of additional areas dealing with the implementation and management of the classification system, whether the current or the proposed system, that require consideration and improvement.

Dissemination Controls-Impediments to Getting Intelligence into the Hands of Customers

A senior intelligence official stated that "the day-to-day most serious problem is that we don't get intelligence to the policymakers in a **way** that they can use it." The issue is not merely that too much information is compartmented, but that intelligence users may be denied timely access to intelligence data and other classified information due to an originator's tendency to include unnecessary control markings.

Four of the standard control markings[6] established by the Director of Central Intelligence for the Intelligence Comrnunity are security controls; two are not.' The Commission recommends that three of the four security control markings be eliminated. They are duplicative, unnecessary, and impede the timely transfer of intelligence to those who need it. WNINTEL (Warning Notice - Intelligence Sources and Methods Involved) is implicit in the specially protected category, ORCON (Dissemination and Extraction of Information Controlled by Originator) is viewed as more of an impediment to intelligence users than a protection for intelligence producers, and all US classified information is NOFORN (not releasable to foreign nationals), unless a decision is made to release such information. Accordingly, the REL TO (authorized for release to. . .) control should suffice.

Under the new classification system, security control markings, apart from REL TO, will not be needed or desirable for generally protected information labeled SECRET, because such information will be under *a* discretionary need-to-know regime. Similarly, security control markings will not be needed or desirable for specially protected information labeled SECRET COMPARTMENTED ACCESS because such information incorporates centralized access controls that already specify the personnel (government, contractor, foreign government) who are to receive the information.

The Commission recommends that the two remaining control markings: PROPIN (PROPRIETARY INFORMATION), and NOCONTRACT (not releasable to contractors or consultants) be combined into a single marking: government-industry-restricted information (GOVIND). The NOCONTRACT marking, as currently used, often prevents contractors from obtaining the information they need to do their job. This is particularly inappropriate in the case of Federally Funded Research and Development Centers (FFRDCs). These are non-profit institutions with no production facilities, no products or services to sell in commercial markets, and that are not supposed to compete with non-FFRDCs. Accordingly, procedures should be developed to routinely obtain advance agreement that corporate proprietary information is given to the government with the express understanding that such information can be shared with FFRDCs as required by the government.

In the system we propose, government employees and contractors will be cleared to the same standard and appropriately indoctrinated. Consequently, there will be no need to restrict information from contractors with a need to know, other than to protect two types of information. The first is information that is provided to the government by a commercial firm or private source under an express or implied understanding that the information will be protected as a trade secret or proprietary data and will not be disseminated to a potential competitor. The second is government information, for example budgetary information, that could give the contractor an unfair competitive advantage. A new marking, GOVIND, would restrict both types of information.

Agency-specific dissemination controls such as "Exclusive For," "Secret/Sensitive," or "Eyes Only" add to the confusion, and are rarely enforced. We recommend that no agency-specific, dissemination-control markings be used for security purposes. There is no consistency between agencies in the terms

used. Whatever unique handling restrictions they imply usually are not understood by the recipient agencies and are improperly applied.

The Commission recommends that, with the exception of "GOVIND" and "REL TO," dissemination markings and controls be eliminated.

Sharing Classified Information

The world is changing and US classified information not only is provided to close allies, but also to coalition partners, some of whom normally have interests quite divergent from ours. The US also finds it necessary to provide classified information to the NATO and the United Nations in circumstances where such information, once provided, may be broadly distributed.

It is not possible to anticipate every situation, and flexibility must be preserved so that military commanders and foreign policy officials are able to meet the special needs and requirements of each situation. Nevertheless, it is helpful to have general governmentwide guidance as to the types of information that readily can be shared or that pose particular problems. This reduces the amount of information that must be assimilated and the number of decisions that must be made on an ad hoc basis in the heat of a crisis.

The security executive committee should review information sharing requirements and ensure that guidance and expertise is readily available to inform and assist officials who must make release decisions.

The Commission recommends development of govemmentwide guidance for sharing classified information with coalition partners and with the United Nations.

Billet and Access Control Policies

One of the most frustrating features of many current SAP and SCI systems is the resourceintensive, bureaucratic procedure for authorizing access. Military commanders and senior managers confront cumbersome approval requirements, often including arbitrary numerical ceilings and rigid billet structures, if they wish to bring another person with a legitimate reason for access into the compartment.

Program managers try to limit the number of people allowed access to many special programs by imposing an arbitrary ceiling on the number of individual billets (spaces) authorized for a particular organization or facility. Both government and industry organizations are forced to resort to inefficient and costly practices to get around the access restrictions to get the job done. The Commission found that the imposition of these numerical ceilings and rigid billet structures does not reduce the actual number of persons accessed nor enhance the security of a controlled access program. Instead, these practices add unnecessary complexity and confusion.

Program managers ty to limit the number of people allowed access to many special programs by imposing an arbitra y ceiling on the number of individual billets authorized for a particular organization or facility.

Because a special access program manager refused to approve a new billet structure with a higher billet ceiling, a government supervisor briefed and debriefed multiple people against a single authorized billet to get *the number* of **people** *needed for the program. The supervisor would brief an engineer, telling the engineer to think abouf a particular controlled access issue, then immediately debrief him/her. The same procedure was followed wifh other needed personnel until all had been briefed on the controlled access program, given a problem to resolve under fhe program, and then debriefed. Several weeks later, the supervisor used the same brief/debrief method to obtain fhe solutions from the personnel.*

The number of persons accessed to specially protected information should be based on the number necessary to accomplish the job.

These controls only give the illusion of security while adding excessive cost and inefficiency to the access approval process. The Commission, then+ fore, recommends an end to the practice of limiting access to specially protected information based on the number of authorized billets or imposed numerical ceilings. The Commission believes that, to permit more effective accomplishment of mission tasks, a zero-based review and update of controlled access rosters in concert with using elements is necessary to determine the personnel who truly have a bona fide contractual or job-related requirement for controlled **access** information. The results of the review should form the backbone of new access management processes that should eventually feed into a data base system. Quite simply, the number of persons accessed to specially protected information should be based on the number necessary to accomplish the job.

The Commission recommends that the Secretary of Defense and the Director of Central Intelligence direct that controlled access program managers conduct a zero-based review to ensure that all personnel with a mission-essential need to know specially protected information receive access to the information. The number of accessed personnel should meet the need for properly cleared and indoctrinated persons to support acquisition, planning, and operations and not depend on arbitrary ceilings.

Secrecy Agreements

At present, most US Government employees and contractors granted access to classified information sign a Classified Information Nondisclosure Agreement (Secrecy Agreement) in which they agree never to divulge classified information to an unauthorized person. While this agreement does not contain a prepublication review provision, the individual agrees that, if there is uncertainty about the classification status of information, he will confirm with an authorized official that the information is unclassified before he discloses it.

Recipients of access to Sensitive Compartmented Information (SCI) and DoD Special **Access** Programs (SAPs) sign a nondisclosure agreement or indoctrination statement with a prepublication requirement each time that they are admitted to a compartment, program, or category of information within a program.

The SCI agreement obligates the signer not to disclose anything marked as SCI or that they know to be SCI, and to submit for review any material that "contains or purports to contain any SCI or description of activities that produce or relate to SCI, or that they have reason to believe are derived from SCI." Recipients of National Security Agency information agree to submit for review all information that contains or purports to contain, refers to, or is based upon "Protected Information," essentially defined as classified information obtained as a result of their relationship with the NSA.

Recipients of DoD SAP information sign a similar agreement that indoctrinates them into the program and obligates them to submit for review all information which contains or purports to contain any "Designated Classified Information," (essentially defined as SAP information) or description of activities that produce or relate to Designated Classified Information.

Central Intelligence Agency employees sign a secrecy agreement that contains a significantly broader prepublication agreement that obligates them to submit for review any material they contemplate disclosing that contains any mention of intelligence data or activities or contains any other information or material that might be based upon classified information. There are strong arguments for this expansive language. It has more teeth and gives broader legal protection. because the obligation is not limited to classified information, the government can proceed against the individual simply for failing to submit for prior review information that mentioned or was based on intelligence without having to prove classification.

Most of the Commissioners are not persuaded that persons with access to the same classified information should have differing obligations. Most Commissioners also are not persuaded that intelligence professionals at the CIA should be held to a higher standard than that applied to others in government who receive CIA information. These Commissioners do, however, acknowledge that it is not unreasonable for a Director of Central Intelligence to conclude that CIA employees should be held to a higher standard because, for example, CIA employees are more likely to be exposed to sensitive sources and methods information over their career than many employees in other agencies.

Prepublication review is designed to guard against the malicious and the uncertain. Those with malicious intent will not submit material for review no matter how broad the standard. The conscientious employee or retiree, uncertam as to whether information is classified, will submit material even with a narrow standard. The Commission is concerned about the chilling affect of any prepublication review, but particularly the broad standards in the current CIA secrecy agreement. Government employees should not forfeit the ability to participate in public policy debates merely because they have, or had, access to highly classified information. Indeed, their participation in the debate should be encouraged. On bai ance, the majority of the Commissioners concluded that there should be one andard secrecy agreement for government and contractor employees wit access to compartmented information that does not incorporate the higher review standard in the current CIA version. However, the Commission also recognizes that the Director of Central Intelligence may conclude that his statutory responsibility to protect sources and methods requires that he maintain the stricter version.

Standardization of secrecy or nondisclosure agreements and of prepublication review requirements is needed.

Regardless of the prepublication review standard, the Commission believes that it is neither legally required nor desirable, with respect to SCI and SAP material, for the individual to sign a separate nondisclosure agreement for each compartment, subcompartment, program and category of information within a program. A single secrecy agreement obligates the individual not to disclose classified information. A single prepublication provision obligates the individual to submit specially protected material for review. Although there is no harm in reminding an individual of his obligation to protect the information, the multiple forms may in fact create the erroneous impression that unless a new form is signed for each type of information 'or for each compartment, the obligation to protect the information and submit it for prepublication review is somehow not present. Moreover, there are costs involved in producing, using, and storing the plethora of forms, particularly in an environment in which many individuals have multiple **accesses. These** costs can and should be avoided.

The Cornmission believes that standardization of secrecy or nondisclosure agreements and of prepublication review requirements is needed.[8] Two agreement forms should suffice: one agreement for generally protected information, and one for specially protected information. If an individual signs the agreement for specially protected information, it will be the only agreement required.

The Commission recommends that no individual sign more than two nondisclosure agreements. One standardized agreement, without a prepublication review provision, will be used for generally protected information; the other standardized agreement, with a prepublication review provision, will be used for specially protected information. If an individual signs the agreement for specially protected information, signing an agreement for generally protected information would not be necessary.

Declassification

Simply put, the current system for declassification does not work Much of the information that is classified does not have a declassification date. Generally it is marked OADR (Originating Agency's Determination Required) and remains classified indefinitely. Detailed review of these documents is not feasible, and arbitrary bulk or automatic declassification schemes are perceived as risking the loss of information that still requires protection.

The Cold War period produced a huge amount of classified information, and thus, an enormous backlog of potentially declassifiable information. In addition to information held by individual agencies, there are an estimated 300-400 million pages of classified information in the National Archives. Millions of additional documents are classified each year. The Information Security Oversight Office reports between 6-7 million original and derivative classification actions per year in Fiscal Years 1990 to 1992.

Agencies generally are not willing to declassify information without review, yet as the mountain of classified information grows, it is clear that a

line-by-line and document-by-document review of this information would be extremely expensive and time consuming.[9] Moreover, given public and congressional concern today that sufficient resources are not being devoted to current FOIA, Privacy Act, and mandatory review requesters, diverting limited available resources to a time-consuming review process that is not driven by customer demand is unacceptable.

Any declassification regime, therefore, must be examined to ensure that it does not create a significant burden for government agencies without providing any great advantage to the public. Put more positively, a new classification system should maintain classification for the shortest possible time and make the declassification system more efficient rather than more costly.

We believe that a great deal of information can be automatically released in ten years and that most information can be released in 25 years. What is necessary, however, is to distinguish those categories of information that are good candidates for declassification after 10, 15, or 20 years from categories of information, such as human-source information, that may require protection for longer periods of time. By correctly categorizing classified information, we can reduce the number of times that the government needs to review documents and develop a strategy that will allow release of information without the need for line-by-line review.

We recommend that a new Executive order on classification specify certam categories of information that can be exempted from automatic declassification at the end of 10 years, and also permit agency heads to nominate, and the security executive committee to approve additional limited categories of information that may require protection longer than 10 but fewer than 25 years. Information could then he marked at the time of its creation to reflect a date upon which it would be automatically declassified.

For example, if it were believed, with respect to a particular category of information that, at the end of 10 years, classification would have to be extended for the majority of information in that category, a longer time period would be selected. Otherwise, when the IO-year, automatic-declassification date arrived, the agency would feel compelled to do a line-by-line review of the information, most of the information probably would remain classified, a great deal of cost would be incurred, and little advantage would be derived by the public.

On the other hand, if it were believed that most of the information in that category could be released at the end of 15 years, then it would be expected that when the automatic declassification date arrived, the agency would feel more comfortable adopting a risk management rather than a risk avoidance approach to the material. The agency would be far less likely to see the need for line-by-line review of the information and far more willing to release the information with little or no review. For example, if it were believed that finished intelligence could be released in 15 years, then it could be expected that at the end of that period reviewers might conclude that the release of 15-year-old political intelligence would not result in significant harm, that the release of E-year-old economic intelligence would not do significant harm, but that there were a couple of weapon systems still in use and still of continued interest. In such a scenario, reviewers might look to see if S-year-old military intelligence written on these two weapon systems still should remain classi-

Any declassification regime. . . must . . . ensure that it does not create a significant burden for government agencies without providing any great advantage to the public.

fied, but would not undertake a line-by-line review of the rest of the 15-year-old finished intelligence.

We are keenly aware that an important underpinning of our system of government is an informed citizenry and that without the prompt release of pertinent information, intelligent public policy debate, academic discussion, and historical research is handicapped. Nevertheless, there are clear examples where the American people are better served by continued protection of certain classified information. For example, the revelation of the identity of a confidential intelligence source, even after the passage of years, can have a serious negative impact on that individual and would not serve US interests. Similarly, release of information about a previous generation of US weapons can still have a significant negative impact on the safety of US forces.

- We believe the proper balance can be struck in the Executive order by allowing agency heads to exempt, at the time of its creation, specific information from the 25 year automatic declassification. This information would be within the following categories:

- Information that would jeopardize a human intelligence source or impair use of an intelligence method.

- Information that would compromise sensitive military operations.

- Information that would impair US cryptologic systems or activities.

- Information about **weapons** technology that provides the US with a battlefield advantage or would assist in the development or use of weapons of mass destruction.

The Commission recommends that four principles drive the declassification **system:**

a) A classifier should attempt to identify a specific date or event when information can be declassified.

b) If no date or event is specified, there is a rebuttable presumption that all classified information would be declassified no later than 10 years from the date of creation.

c) The Executive order should specify categories of information, exempt from the 10 year declassification requirement, that can remain classified for 25 years. Agency heads should prepare guidelines to implement exemption of these categories. These guidelines will be approved by the security executive committee.

d) The Executive order should also specify very narrow categories of information that will be exempt from the 25 year automatic declassification requirements. These categories should include information that would **jeopardize a human intelligence source or compromise ongoing sensitive military capabilities. Heads of agencies should develop guidelines that will implement the exemption of these categories from automatic declassification. These guidelines would be approved by the security executive committee.**

Making the Classification System Really Work—An Integrated Approach with Appropriate Oversight

The one-level classification system with two degrees of protection is designed to provide a framework that will support a coherent and consistent governmentwide approach to both classification and security. It recognizes that classification drives security costs and that security practices are evolving naturally, albeit slowly, around two levels of protection. It and the other classification management recommendations build upon steps already taken by, and borrow from the ideas of, thoughtful security professionals.

Nevertheless, no system can be expected to work very well if there is no one in charge. Today, there are few govemmentwide standards and, even when standards are supposed to have general applicability, they often are translated and interpreted in ways that do violence to the concept of standardization. Often there is no penalty for noncompliance. Moreover, we conclude that the Information Security Oversight Office (ISOO) simply is not positioned to ensure compliance. Without an effective policy and oversight structure, no coherent security policy is likely to evolve. Instead, inconsistent rules will continue to be formulated, and disputes will continue to impede the development of a uniform policy.

The proposed security executive committee, on the other hand, would be positioned to provide effective centralized oversight. Its staff could include a strengthened ISOO, headed by a security ombudsman, with a broader security oversight role. In addition, the outside security advisory board we propose would provide a mechanism for nongovernment and public interest concerns about the system to be raised to the committee.

Although centralized oversight is a necessary and important innovation, effective oversight must begin at the **agency** level. We recommend, therefore, that each agency appoint a classification ombudsman whose mission is to encourage and act on complaints about over-classification. The ombudsman also will be required to routinely review a representative sample of the agency's classified material. This individual would have the authority to ask why a particular piece of information was classified and to order it declassified if no persuasive reason is forthcoming. Real-time review of employee complaints, cable traffic, and other documents; real-time identification of categories of information subject to misclassification; and real-time identification of the individuals responsible for classification errors would add management oversight of classification decisions and attach penalties to what too often can be characterized as classification by rote. The system outlined above, in its broad contours, has been in place in the Department of State for the past two years, and we are told that over the past six months noticeable progress has been made. Information that previously had been classified is no longer classified and greater discipline has been injected into the entire classification process.

The Commission recommends:

a) Strong centralized oversight by the security executive committee as well as more effective oversight at the agency level.

b) A strengthened Information Security Oversight Office as a part of the security executive committee staff.

c) A requirement that each agency appoint a classification ombudsman, establish a hot line for employee classification questions and complaints, and institute a spot check system.

Increased attention must be paid to identifying and protecting sensitive but unclassified information within the Defense and Intelligence Communities.

Dealing with Sensitive but Unclassified Information

The information universe usually is subdivided into classified and unclassified, with best estimates of the ratio having classified as about ten percent of total government information. Unclassified information is further subdivided into sensitive information-unclassified information which has some confidentiality requirement-and non-sensitive information which may be disseminated freely. It has been estimated that as much as seventy-five percent of all government-held information may be sensitive.

Government-held sensitive but unclassified information is information whose loss, misuse, unauthorized access to, or modification of, could adversely affect the national interest or the conduct of Federal programs, or adversely affect the privacy to which individuals are entitled under the Privacy Act.

As with classified information, this information must be protected to ensure its confidentiality, integrity, and availability. In some cases, we do not wish unauthorized persons to see certain information, such as medical or personnel records. Sometimes, it is more important that information is not changed or destroyed, such as with payroll or other payment records. Finally, it may be important to ensure the availability of these records within the period of time necessary for their particular use or application. For example, if a system were intentionally clogged or disrupted, we might be unable to access treatment data to deal with a medical emergency or logistics data to deal with a military or diplomatic crisis.

The Commission believes that our information infrastructure is at increasing risk, but its vulnerability is not sufficiently understood or appreciated and there is not in place a process to appropriately deal with the problem. Increased attention must be paid to identifying and protecting sensitive but unclassified information within the Defense and Intelligence Communities. In addition, the information system security countermeasures that are developed should be available more broadly to protect such information in the rest of the government, as well as information that, while neither classified nor government-held, is crucial to US security in its broadest sense. We have in mind information about, and contained in, our air traffic control system, the social security system, the banking, credit, and stock market systems, the telephone and communications networks, and the power grids and pipeline

networks. All of these are highly automated systems that require appropriate security measures to protect confidentiality, integrity and availability.

The Commission recommends that the Secretary of **Defense and the Director of Central Intelligence put in place a process to evaluate the vulnerability of sensitive but unclassified information within the Defense and Intelligence Communities and to explore appropriate countermeasures.**

Chapter 3.

Threat Assessments-The Basis of Smart Security Decisions

A critical element necessa y to make smart security decisions is reliable, usable, intelligence data defining the threat.

Asleep at the Wheel

While our broad national security agenda helps set the stage for determining what to protect, the actions of other states and individuals define more precisely where security must be focused. The Commission has frequently been reminded that the United States is the single biggest intelligence target in the world. Traditional, long-range intelligence threat predictions are now of reduced value in a world of evolving alliances and volatile political, socioeconomic, cultural, and regional crises.[10] Threats must be reassessed frequently. The Commission found many instances, discussed throughout this report, where security countermeasures currently employed appear to be excessive in terms of the threats or are not linked to threats at all.

A critical element necessary to make smart security decisions is reliable, usable, intelligence data defining the threat. Currently, there are efforts underway in the Defense and Intelligence Communities to incorporate threat assessments when developing security policies. For example, the DOD'S Acquisition Systems Protection Program (ASPP), designed to protect leading-edge technology, calls for incorporating threat assessments in each phase of advanced weapon systems development. Defector information and espionage lessons learned are taken into account in updating personnel security procedures. Physical and technical security policies and countermeasures, traditionally based on vulnerability assessments, are now being developed using threat information. As a result, security policies are being revised and dramatically changed. The Commission applauds these efforts.

However, getting from the Intelligence Communityspecifically the counterintelligence organizations-the threat information necessary to sup port coherent, risk-based security countermeasures policies, military operations, and industry is an ad hoc rather than a systematic process. In the absence of access to threat assessment information, security policies have been based on risk avoidance, constrained primarily by the availability of resources.

The reasons for the failure to incorporate intelligence and counterintelligence information into security policies are numerous. Traditionally, the intelligence and counterintelligence communities have been separate and distinct from their security counterparts. Intelligence and counterintelligence activities are discrete programs where budgets are built and justified in terms of collection and production against specific targets. Security programs, on the other hand, are normally funded from base operating or administrative funds of various agencies and are difficult to link to specific programs. These pro-

grams and funds, when accounted for at all, generally have not had to face the scrutiny of cost-risk analysis (with some individual exceptions).

Security officials do not always know how to task the Intelligence Community for threat information. They have neither the necessary clearances and contacts within the Intelligence Community nor an understanding of the contribution that intelligence producers can make. The counterintelligence community, for its part, focuses on its mission of conducting investigations and collecting, analyzing, and exploiting information to identify and neutralize the intelligence activities of foreign powers that adversely affect US national security. Yet the security policy community has not been viewed as a primary customer. Consequently, intelligence and counterintelligence requirements are not defined to support rational security decision making. The Commission believes that the security community must work closely with the National Advisory Group for Counterintelligence and the newly appointed Issue Coordinators to develop collection and production strategies that address security consumers needs.

Security officials do not always know how to task the Intelligence Community for threat information.

When security officials do task for threat information, support is not always timely and frequently is overclassified. Department of Defense customers often wait months while counterintelligence requirements are forwarded through several operational levels for approval, and to service headquarters elements for validation. The requirement is then forwarded to analysis centers for drafting, which requires an additional 120 days. Some DoD personnel reported to the Commission response times longer than a year for critically needed requests. Roadblocks are also encountered if classified information needs to be disseminated in an unclassified form. The counterintelligence community seems unable to provide unclassified analyses.

> *One senior DoD official requested an unclassified report to use in a contractor security awareness briefing. The report arrived six months later—stamped* ***Secret,*** *Not* ***Releasable to Contractors.***

In the absence of a comprehensive threat assessment process, some security organizations have performed their own. The Air Force's Special Access Program (SAP) has created dedicated analytic cells to provide timely assessments. Air Force SAP intelligence specialists directly contact the scientific community and perform independent assessments on cutting edge Air Force technologies and developmental weapon systems. Navy and Army SAP programs draw upon cleared service analysts. Not possessing a cadre of analysts, DoD field elements postulate the local threat using worst case scenarios until finished assessments arrive. This results in employing stringent, expensive countermeasures to prevent the loss of critical technologies information. The field elements note that when the much awaited reports do show up, they are either too general to be applicable, or they contradict other services or the Defense Intelligence Agency's assessments, often regarding the same technology.

> *A DoD program manager requested an assessment of the foreign intelligence threat to a city, with particular emphasis on whether* there *was targeting of the advanced technology system that was being developed at a facility. Eighteen months later, the program manager received from one DoD element an assessment, stating that the threat to his area was low, with no particular foreign interest in the technology. Another DoD element had already informed him, six months earlier, that there was an established,*

aggressive foreign intelligence collection program targeting the developing technology.

There is a schism concerning threat information between security policy officials and the Intelligence Community that widens greatly when it comes to a supportive relationship between counterintelligence organizations and security professionals. At the national level, counterintelligence funding is under the purview of the DCI's National Foreign Intelligence Program. But the counterintelligence community is a loose confederation of separate activities held together by budgetary convenience, not centralized management.' The five major counterintelligence organizations (FBI, CIA, Army, Navy, and Air Force) can work together collegially, but frequently strike out on their own. Some of these organizations have difficulty identifying their customers. Indeed, one senior counterintelligence official points with pride to the fact that "we (counterintelligence organizations) are our own best customer." Counterintelligence information is collected, analyzed, produced, and disseminated separately from normal intelligence channels. Critics charge that this process ignores national strategy and policymakers' needs.

There is no common counterintelligence data base . . . from which threat assessments might be drawn.

This fragmented counterintelligence organizational structure has also created large gaps in knowledge. For example, there is no common counterintelligence data base, either within the Department of Defense itself or among the counterintelligence organizations generally, from which threat assessments might be drawn. This shortfall may contribute to the difficulty counterintelligence organizations have had in supporting clearly defined customers, like the National Industrial Security Program (NISP). Despite two years of work by counterintelligence representatives within the NISP, no mechanism was created to communicate threat data to industry.

For senior policymakers, while there is an interagency coordination process to support them, the products fall short. National counterintelligence assessments, such as the "Winds of Change" and the "Triennial Threat Assessment of the Foreign Intelligence Threat and Effectiveness of US Counterintelligence and Security Countermeasures," need to use more current data, be made more policy-relevant, and provide a clearer picture for the reader. As now written, these assessments do not respond, in a timely manner, directly to national-level requirements, aid resource allocation, or meet the needs of program managers and military commanders. Future editions, if any, require a keen understanding of senior policymakers' requirements and tighter analytic presentation and packaging.

The Commission heard from many individuals within the Department of Defense about the need to streamline the counterintelligence structure and we understand that the Deputy Secretary of Defense and the Director of Central Intelligence the are considering options to do this. The Commission believes such restructuring can bring savings and better service, but we would expand the discussion to include the Attorney General and the Director of the FBI so as to incorporate other major counterintelligence organizations.

A Wake-Up Call

Information about the dangers posed by foreign governments and organizations does not come solely from counterintelligence assets. Much of it comes from human sources or defectors, signals intelligence, imagery assets,

our diplomatic corps, and other sources that need to be more actively tasked by security officials. In other areas of intelligence production, consumers have a single place to go for analytic assistance. For example, counterterrorism and nonproliferation consumers have individual points of contact that respond, in a coordinated fashion, to their needs. The DCI's Counterterrorism Center (CTC) and Nonproliferation Center (NPC) personnel reportedly broker timely responses to policymakers' requests. These offices do not compete with established production elements. They serve as facilitators, drawing on information and substantive expertise from within the community.

The Commission recommends that the Secretary of Defense and the Director of Central Intelligence appoint the DCI's Counterintelligence Center as executive agent for "one-stop shopping" for counterintelligence and security countermeasures threat analysis.

The Commission does not intend by this recommendation to create a counterintelligence "czar" or to supplant existing authority for counterintelligence investigations, operations, or the unique, individual analytic efforts in support of specific law enforcement or military operations. Rather, we seek a national-level focal point for threat analysis that is easily accessible by government and industry to support broad security management decisions. This "one-stop shopping" office must operate as a corporate information asset of benefit to all government and industry customers. The Counterterrorism Center customer response office can serve as a model.

We seek a national-level focal point for threat analysis that is easily accessible by government and industry to support broad security management decisions.

While the Counterintelligence Center lacks the expertise in domestic threats that the Federal Bureau of Investigation has, it provides an established, credible intelligence production office with professional analysts able to tap into the full range of intelligence and operational reporting. It also has the most experience in providing analysis for senior policymakers.

However, the Commission notes that the current analytic and community elements of the Counterintelligence Center must expand and change dramatically to include a broader community and industry flavor and to incorporate expertise in the security countermeasures areas that it lacks currently, such as threats to information systems security. The Commission expects that the Counterintelligence Center will draw upon the experience and knowledge of other agencies when preparing responses for risk management decisionmaking and coordinate the products extensively. This includes drawing upon the NSA's and the DISA's ongoing efforts that focus on threats to information systems security. Existing interagency analytic efforts, such as the National Advisory Group for Counterintelligence's Analytic Working Group, will fold into this initiative.

Further, dissemination procedures need to be restructured, allowing customers to pull the information they need from the system, instead of having it pushed to them in restricted formats. Threat information needs to get out to users at all levels in the Defense and Intelligence Communities and in industry.

The Commission is aware of and applauds a recent decision by the counterintelligence agencies to create an interagency data base. However, the data base needs to expand to allow for users with varying classification levels. The

Commission also urges the community to take advantage of the counterintelligence data base program now under **way** within the Department of Defense and ensure that the two data bases are compatible. This interagency data base initiative should be undertaken and a prototype fielded immediately.

The Commission recommends that the DCI's Counterintelligence Center serve as the executive agent to spearhead the rapid creation of a communitywide counterintelligence and security countermeasures data base for government and industry use.

Chapter 4.

Personnel Security— The First and Best Defense

The personnel security system is at the very heart of the government's security mission.

So far as concerns the DoD and the Intelligence Community, the main purpose of personnel security programs is to protect the national security interests of the United States by insuring the reliability and trustworthiness of those to whom information vital to those interests is entrusted. because the government is so completely dependent on cleared personnel to safeguard classified information, the personnel security system is at the very heart of the government's security mission. Without adequate personnel screening, the rest of the security mission would be a worthless facade and a waste of resources. Recent history is regrettably all too rich in proof of the damage that a single cleared person can cause.

The Commission believes that the personnel security program will remain the centerpiece of the Federal security system in the post Cold War era, particularly as we move to a new classification system in which more information is moved out of compartments and made available to greater numbers of people. For this reason, the Commission is recommending enhancements to the personnel security program. These enhancements will result in increased costs, but the Commission believes these costs will be offset by other improvements we suggest.

The process of granting clearances will always be controversial. It makes determinations about security risk by examining personal background information to form a judgment that can have serious consequences for the individual and for the government. There is no perfectly reliable or unarguably correct way to predict whether an individual will become a security problem in the future. In the end, all clearance decisions are judgments, hopefully well informed and carefully made, but nevertheless fallible. From time to time the process will fall short, either to the detriment of an individual when a clearance is denied, or to the detriment of the government when a serious security problem develops.

The Commission finds that the clearance process is needlessly complex, cumbersome, and costly. Security clearances are sought for too many persons who have no real need for a clearance. There are too many different forms in use. There is insufficient automation and little interconnectivity between agencies. Investigation and adjudication are practiced inconsistently among agencies, resulting in reciprocity problems, delays, and increased cost to both government and industry All too frequently clearances granted by one agency are not accepted by another, or even by another program manager within the same agency.

The Commission believes that these shortcomings in the Federal personnel security system can be remedied. Our goal is to establish a security clear-

ance standard the application of which will be tracked in a communitywide data base and will be fully transferable and valid among all government agencies.

THE PROCESS BEGINS

Requesting a Clearance

Except where a clearance is required for initial employment, the clearance process begins when management determines that a worker requires access to classified information or requires the authority to change information or systems in ways which may affect the integrity or availability of information. Management submits a clearance request form, an investigation is conducted, and the results are forwarded to an independent adjudicative center, which determines whether the individual is suitable for a security clearance. Clearance decisions are subject to appeal and review through formalized administrative procedures. The government conducts similar investigations on all Federal civilian employees in the executive branch and on military members to determine whether they are suitable for Federal employment or service. These position suitability determinations differ from clearance decisions in that they are not made according to standardized criteria. Rather, the hiring component, not an independent adjudicative center, makes the determination, and fewer procedures are in place to appeal adverse decisions.

The Commission learned that thousands of costly security clearances are requested annually for persons who do not require actual access to classified information or technology or the authority to modify sensitive information or systems, and who do not otherwise occupy sensitive positions. For example, guards, shipyard workers, various trades craft, and maintenance, custodial, concession, and cafeteria workers are routinely submitted for clearance even though they only require access to a controlled area (facility access) and thus may receive only superficial or inadvertent exposure to classified information. Unfortunately, many of these personnel have complex backgrounds which, when applied against security clearance criteria, require extensive investigation and administrative due process, thereby overburdening an already overtaxed system. This only serves to delay significantly the processing of legitimate requests and increases costs.

Thousands of costly security clearances are requested annually for persons who do not require actual access to classified information

The Commission recommends that clearances be requested only for personnel who require actual access to classified information or technology. For most of those who merely require facility access, a position suitability determination based on the results of a National Agency Check with Inquiries (NACI) should be the maximum allowed.

The Commission found that many managers consider the clearance process slow and inefficient. Because there is no cost incurred for submitting clearance requests, military commanders and program directors often submit an excessive number of clearance requests to ensure that they receive an ade-

quate number of cleared personnel to meet their needs. Investigative and adjudicative organizations, many of which face steadily declining budgets, must accept all requests, resulting in runaway costs and delays throughout the system. A solution is needed that will impose discipline at the requester level, while insuring that the system accommodates essential clearance requests quickly and efficiently.

Industrial finding . . . can impose a sense of cost on agencies that request clearances.

A fee-for-service funding mechanism, such as industrial funding or a revolving fund, can impose a sense of cost on agencies that request clearances. Rather than use appropriated funds, industrially funded agencies charge customers for services provided and finance operations from this income. Fee-for-service operations tend to be more efficient and appropriately scaled to size **because** customers must consider the cost of the service when making requests. For example, the Office of Personnel Management (OPM), which operates on a revolving fund, found that investigative requests steadily decreased after it instituted industrial funding. Similar decreases in clearance requests would likely occur with the adoption of an industrial funding mechanism throughout the DoD and the Intelligence Community (to include industry). Fee schedules could be developed that would allow agencies and organizations requesting clearances to trade off the advantages of expedited processing **against** higher costs. The **Commission recognizes** that converting to a new funding strategy cannot be accomplished overnight. However, we believe that it is time to begin purposefully moving towards this new **strategy.**

The Commission recommends that fee-for-service mechanisms be instituted to fund clearance requests within the DoD and the Intelligence Community.

Rescreening and Fairness

Rescreening is the process of assessing the likelihood that individuals will be cleared before they are formally submitted for a clearance. It generally involves the completion of a personal history statement or security questionnaire and/or interviews with the subject or supervisors. Prescreening saves a considerable amount of time and money by insuring that only those individuals with a reasonable chance of obtaining a clearance are submitted for processing. All agencies in the DoD and the Intelligence Community prescreen applicants to some degree. For example, in the DoD, prescreening is conducted at military enlistment centers and on all persons considered for SCI access. The effectiveness of this program is evident in the very low clearance denial rates for these individuals.

The Commission learned that substantial problems may develop if government organizations ask private firms to prescreen their own employees for a security clearance. Such firms are concerned about legal liability if they conduct prescreening as agents of the government. Contractors may interpret the relevant security standards differently and are not able to waive the standards as do government organizations. Consequently, qualified individuals may needlessly be denied an assignment or even employment. Further, if the contractor performs the prescreening of its own employees instead of the government, those eliminated have no appeal rights.

Furthermore, suggestions have been made that some firms use the clearance process to weed out employees that they consider unsuitable. For example, government investigators conducting background checks sometimes find that the subject's managers and supervisors will not recommend the subject for clearance, In other cases, investigators discover that the individual whose name was submitted for clearance is not scheduled to work on a classified contract. In these instances the clearance denial can afford the contractor a convenient explanation for terminating the individual's employment. The Commission believes that it is the obligation of the contractor to nominate individuals who enjoy the full support of management within the firm.

The Commission recommends that formal prescreening of contractor personnel be **solely performed** by the **government** or **an** independent company hired by the government specifically for that purpose, not by the company that employs the personnel.

Some special access programs have prescreened individuals without their knowledge or consent.

While most prescreening programs appear effective in weeding out problem cases, some special access programs have prescreened individuals without their knowledge or consent. While this practice is not widespread, it may result in adverse employment consequences and deprive the person of knowing the rationale for the employment consequences or having the right to appeal. The Commission believes that unconsented prescreening should not be conducted unless warranted by extraordinary circumstances, such as cover or counterintelligence operations.

The Commission recommends that within the DoD and the Intelligence Community, individuals (including employees of contractors) considered for a contractual or employment related security clearance or access may be formally prescreened only with their full knowledge and consent, unless conducted pursuant to procedures approved by the security executive committee.

Forms and Automation-Ending the Paper Trail

The Commission found that there are literally hundreds of different forms designed to establish clearance and access eligibility. For example, there are over 45 different prescreening forms in use throughout the government and industry, all of which request essentially the same information. Individuals must often complete several such forms to obtain access to different programs, resulting in delays and ultimately in increased costs.

A number of forms and personnel security questionnaires **are** used to apply for security clearances. None are accepted laterally. Currently the Office of Management and Budget (OMB) supports the establishment of a single form for all positions in government that require a clearance or are otherwise designated as sensitive. The NISP has developed such a standard form to replace all other personnel security questionnaires, but it has not yet been adopted. Until a standard government form is adopted, the Secretary of Defense and the Director of Central Intelligence should require that all inves-

tigative agencies within the DoD and the Intelligence Community reciprocally accept the government approved personnel security questionnaires of other agencies.

The Commission recommends that:

a) The personnel security questionnaire devised by the NISP be adopted for **use throughout the Department of Defense and the Intelligence** Community.

b) A standard prescreening form be developed for use throughout the Department of Defense and the Intelligence Community.

The Commission supports the development of standardized forms in an electronic format as a way to facilitate reciprocity and reduce costs. Currently, most clearance request forms and questionnaires are paper-based. Accordingly, handling times add weeks to the process of conducting background investigations. Moreover, as many as 30 percent of these questionnaires are rejected due to missing or incomplete data, adding as much as three months to the clearance process and thereby driving up costs. Significant savings will be realized when personnel security questionnaires are developed in an interactive, electronic format that guides the completion of each response and ensures that only fully completed forms are submitted. The Commission believes that automation is crucial to improving efficiency and responsiveness throughout the **clearance** process. Examples of ongoing and needed initiatives include:

The Commission believes that automation is crucial to improving efficiency and responsiveness throughout the clearance process.

- The CIA and the OPM have issued laptop computers to field investigators so that field reports can be submitted electronically rather than dictated and typed at separate locations.

- Some agencies are exploring the use of computer administered security interviews as a way to gather information from subjects in a more cost effective manner. Computer administered interviews cost as little as $20 to $30 per interview, versus up to $200 for a subject interview.

- Military members frequently arrive at assignments without the required security clearance, driving up costs as they await clearances to perform duties. One adjudicative organization has proposed that linkages be developed among investigative indices, adjudicative data bases, and personnel data bases, forming an electronic **data** interchange that would ensure almost **all** military members arrive at their next assignment with clearance in hand.

The Commission recommends that the Secretary of Defense and the Director of Central Intelligence invest in automation to increase timeliness, reduce cost, and improve the efficiency of the entire personnel security program.

INVESTIGATIONS-ASSESSING TRUSTWORTHINESS

In 1993, the DoD accounted for the majority of cleared personnel in the Federal Government: about 60 percent of the over 800,000 individuals cleared to the Top Secret and SCI levels; 97 percent of the 2.24 million individuals cleared to the Secret level; and 99 percent of the 151,000 cleared to the Confidential level. With such a large number of cleared personnel, any attempt to increase investigative requirements for the DoD will result in substantial cost increases.

Currently, Federal agencies conduct more than 15 types of investigations. However, the majority fall into the following three categories:

- The National Agency Check (NAC) or Entrance National Agency Check (ENTNAC), which involves records checks of national law enforcement and government agencies.

- The National Agency Check with Inquiries (NACI), which includes the records checks described above plus written inquiries to local law enforcement agencies, former employers and supervisors, listed references, and schools attended in the previous five years.

- The Single Scope Background Investigation (SSBI), which is a full field investigation with a scope of 10 years that includes the checks described above plus credit checks, subject, reference, and neighborhood interviews, as well as verification of birth, citizenship, education and employment.

Investigative Requirements-Streamlining the Process

In 1991, National Security Directive 63 established the SSBI as the single investigative requirement for access to Top Secret and Sensitive Compartment Information throughout the Federal Government. A IO-year scope was adopted as a compromise between the 15-year scope of the special background investigation and the five-year scope of the background investigation. While not required by DCID 1/14, certain agencies and programs augment SSBIs with some form of screening polygraph.

NSD 63 ordered that SSBIs would not be duplicated and would transfer between agencies. However, some agencies, citing variability in investigative quality, take advantage of a loophole in NSD 63 to "upscope" investigations conducted by other organizations. The variability in the quality of investigations stems from differences in use of telephone interviews (considered a substandard practice by many), number of sources contacted and number and diversity of developed leads pursued. Some agencies report results in full, detailed narratives while others use summaries. These inconsistencies serve as an obstacle to reciprocity and add to processing delays.

The Commission believes that the SSBI is a reasonable investigative requirement for access to specially protected information under the new classification system. However, it can be made more efficient by refining the scope and eliminating unproductive leads that are expensive and costly to develop. A 1991 study by the DCI's Personnel Security Working Group (PSWG) determined that 90 percent of adjudicative issues are developed within a seven year scope. Moreover, the Commission learned from the investigative com-

munity that requiring investigators to interview neighborhood sources at every residence and to conduct education and birth record checks in person is costly, time consuming and rarely elicits significant adjudicative information. They suggest that refining the SSBI to address these concerns will drive down costs without affecting the quality of the investigation. For example, subjects could be required to provide verification of birth and education rather than using investigative time to pursue these leads.

Currently, there is no common investigative requirement for Secret or Confidential access in the Federal Government. Military enlisted personnel. and officers, upon entry into the military, receive some variant of a **NAC** that serves as the basis for granting Secret and Confidential clearances. This is the lowest investigative requirement in government. Federal civilian employees are granted Secret and Confidential access on the basis of a NACI or a limited background investigation.

As the Commission proposes to downgrade a significant amount of information from higher to lower levels of protection, we are concerned by Intelligence Community representatives who have stated that they will oppose downgrading information if the only investigative requirement for generally protected access is a NAC. They do not believe that the NAC provides an adequate assessment of trustworthiness or reliability. The Commission concurs and believes that the only way to move more information out of compartments, thereby increasing its availability to customers, is to increase the investigative requirement for access to classified information that is generally protected.[11]

The Commission found substantial support. . . for increasing the Secret clearance requirement to a NACI plus credit check.

The Commission found substantial support in the Defense and Intelligence Communities for increasing the Secret clearance requirement to a NACI plus credit check. The Stilwell Commission and the NISP made similar recommendations. While this initiative will increase the cost of each **investigation** by 50 percent (from $48 to $72)[12], offsets will be realized through an overall reduction in the number of individuals who undergo full field investigations and reinvestigations and operational economies derived through greater availability of needed classified information to the customer community.

The Commission recommends:

a) The investigative standard for a Secret Compartmented Access clearance be an SSBI with a scope of seven years. Moreover, investigators should not be required to conduct education and birth record checks in person or neighborhood checks other than the most recent residence of six months or more.

b) The investigative standard for a Secret clearance be a NACI plus credit check, **with expansion as appropriate to follow up only on issues likely to result in adverse adjudication.**

Continuing Evaluation—Reinvestigations and Safety Nets

The personnel security program continually assesses the integrity and trustworthiness of the cleared work force through periodic reinvestigations. US espionage cases over the last 20 years have shown that most damage to national security is caused by already cleared personnel, those insiders who

volunteer to sell or give classified information to foreign governments. Very few applicants intend to commit espionage at the time they seek employment. Currently, individuals cleared to the Top Secret or SCI levels are reinvestigated every five years, and some agencies or programs may require a screening polygraph. Those cleared to the Secret or Confidential levels are reinvestigated every 10 years, although the DoD, with over 2 million cleared personnel, is only current to 15 years.

The Commission believes that current reinvestigation policies should be refined to increase efficiency. For example, an aperiodic reinvestigation interval would offer a greater deterrent effect and provide agencies with more flexibility to focus resources on priority investigations. Adjudicative facilities also have indicated that, based on revocation experience, a seven year reinvestigation interval for **a** Secret Compartmented **Access clearance** and **a 10-year** interval for a Secret clearance are the most efficient.

The Commission recommends that:

a) The reinvestigation standard for a Secret Compartmented Access clearance be an SSBI. Reinvestigations will be conducted on an aperiodic basis, but not less than once every **seven years.**

b) The reinvestigation standard for a Secret clearance be a NAC, local agency check and a credit check. Reinvestigations will be conducted on an aperiodic basis, but not less than once every 10 years.

While reinvestigation provides an important way to monitor the integrity of the work force, safety nets are also needed to ensure that personnel **do** not become counterintelligence risks after they obtain a clearance. Studies have shown that many American spies in the 1980s turned to espionage as a way to resolve personal problems or crises. Some were disgruntled workers who wanted to strike out at the system for perceived injustices, some were faced with pressing financial problems, others were struggling with conflict-ridden family situations and still others had alcohol or drug abuse difficulties. Many saw espionage as the only way to resolve their problems. They volunteered to sell or give classified information to foreign governments after convincing themselves that they could spy safely and not be detected.

Safety nets are also needed to ensure that personnel do not become counter-intelligence risks after they *obtain a clearance.*

While only a very small percentage of employees with personal problems become involved in espionage or other serious security transgression, the damage that can be caused by even one person with sensitive access serves to illustrate the value of programs that help employees resolve personal problems. A few convicted spies have stated that at the time they began spying they were emotionally distraught and in need of counseling. Employee **assistance** programs provide short-term counseling and referral services for **a** variety of problems, including financial, family, vocational, emotional, and substance abuse. Recognizing the value of these programs in increasing worker productivity, many private corporations and some government agencies have established Employee Assistance **Programs** or contract out for these services. National security organizations have an even greater stake in insuring that such services are available to their employees.

The Commission commends those agencies that have established Employee Assistance Programs **and recommends that all agencies in the Defense and Intelligence Communities ensure that similar programs or contractual services are available to employees, particularly those with access to specially protected information.**

Delays in the investigative and adjudicative process contribute directly to customer and government costs.

Clearance Processing-Time Is Money

Delays in the investigative and adjudicative process contribute directly to customer and government costs. As far back as 1981, the General Accounting Office (GAO) reported to Congress that nearly a billion dollars was wasted annually because of investigative backlogs at the Defense Investigative Service. The GAO recommended solving this "$980 million problem" by increasing appropriations for the DE by $12.5 million.

The Commission found that there is no performance standard for timeliness in completing investigations and adjudications. The Commission repeatedly heard from the customer community that 90 days is an appropriate standard for completion of the average investigation and adjudication (65 days for the investigation). However, the DIS, which has contended with declining resources, completes SSBIs in an average of 149 days (including about 40 days for conducting overseas leads) and does not charge a fee. The OPM completes SSBIs in 35, 75 or 120 days, and charges a variable fee. A major SAP uses a private firm that completes investigations in an average of 34 days but, if directed, terminates some cases when significant adverse information is developed. While private firms cannot handle a substantial volume at this time, contracting out investigations in special circumstances, such as priority cases, may enhance competitiveness and further lower cost by preventing the development of backlogs and delays.

The Commission found that several adjudicative organizations were quite timely in their processing. Others, however, required as much or more time to complete the adjudication than was expended on the investigation. Processing and appellate review of individuals facing a possible loss or denial of a clearance also range in processing time from 120 days at one organization to two years for organizations that offer an evidentiary hearing. The Commission believes these areas are particularly amenable to cost savings through process improvement.

The cost directly attributable to delays in the investigative process in FY 1994 could be as high as several billion dollars (assuming that the DoD incurs an average cost of $250 per day beyond the 90-day standard for each worker who is unable to perform his/her duties while awaiting a security clearance). In addition, the DIS is scheduled to take further cuts through FY 1999 that will substantially increase average investigation completion times, resulting in additional billions of dollars in lost productivity as workers are assigned other suboptimal duties while awaiting clearances.

Delays in the clearance process also contribute to increased costs for industry. In today's difficult contracting environment, many firms that do not

hold classified contracts on a continuing basis are handicapped in pursuing new contracts because clearance eligibility lapses on key personnel. A six- to nine-month delay can result while contractors await clearance revalidation. Should the contract involve state-of-the-art battlefield technology, this loss in time could equate to a loss of life for our forces. Waiting time for personnel involved plus delay in contract deliveries amounts to a significant cost to the American taxpayer.

A private firm with government contracts reported that it has 57 employees in the Washington, DC area who have been waiting six to nine months for clearances at a cost to the company, and ultimately the government, of approximately $2.6 million.

A six- to nine-month delay can result while contractors await clearance revalidation.

The Commission recommends that:

a) All investigative, adjudicative, and appellate organizations begin an orchestrated process improvement program with the goal of continuing to ensure fairness and quality while vastly improving timeliness.

b) Standard measurable objectives be established to assess the timeliness and quality of investigations, adjudications, and administrative process and appeals performed by all such organizations within the DoD and the Intelligence Community.

c) As long as an individual has been investigated within the last 10 years, interim clearance at the previously maintained level may be granted based upon a favorable review of a personnel security questionnaire.

d) Standard interim access procedures be established throughout the community for those not previously cleared to the generally protected and specially protected levels.

ADJUDICATION

Adjudicative Standards and Criteria

Adjudication is the process of determining whether an individual meets established criteria for access to classified information. Once a background investigation has been completed, the entire investigative packet, including records of any prior investigations, are forwarded to an adjudicative center. An adjudicator determines whether problem behaviors are present, and, if so, whether the behavior is severe enough to warrant a denial or revocation of a security clearance. Factors that enter into the decision include the seriousness, recency, frequency, and motivation of the behavior as well as any mitigating factors.

The Commission reviewed the adjudicative criteria used in the DoD and the Intelligence Community, visited adjudicative and appellate operations, met with senior officials regarding their adjudicative philosophy and sought the basis for a number of adverse adjudication2 occurring in the past 5 years that have resulted in public controversy. The Commission notes that virtually

all of the adverse adjudications that have resulted in recent public or congressional outcry appear to have occurred in either special access or special intelligence programs at a time when very limited procedural safeguards were made available to personnel working within such programs. In October 1993 the last of these programs instituted procedural safeguards for those who face denial or revocation of their special access. Those safeguards, discussed below (see pp. 55-65), should provide much better protection, but the Commission remains concerned about the lack of reciprocity of adjudications. Efforts are underway to establish standard adjudicative criteria for the entire community and these must be brought to fruition.

As a result of a few *questionable decisions, various special access programs and Federal agencies have developed a wholesale distrust of the industrial clearance process, leading them to readjudicate these decisions.*

The Commission also believes that the security executive committee should, as a first priority, develop a single governmentwide standard for granting security clearances for both Secret and Secret Compartmented Access. This common standard should eliminate the lack of reciprocity among government agencies and between the government and contractors.

The process of developing common standards should also address concerns that have been expressed by civil liberties groups and others as to whether the criteria strike the right balance between the government's need for security and the rights of the individual. The Commission is pleased to observe that such issues as sexual orientation no longer are per se bars to clearance or access. In this regard, the Commission notes that the Attorney General recently issued a statement on nondiscrimination in employment within the Department of Justice and the FBI issued investigative guidelines and security clearance adjudication guidelines. The Commission has not had an opportunity to consider these guidelines in depth, but believes that the principles expressed in these guidelines could be the basis for governmentwide standards.

There are two sets of adjudicative criteria in the DoD and the Intelligence Community. A Director of Central Intelligence Directive (DCID) contains the adjudicative criteria for SCI determinations. While SAPs do not usually require access to SCI, they may require that personnel meet at least the DCID criteria. A DoD regulation contains the adjudicative criteria for Confidential, Secret, and, Top Secret for the military.

The NISI' has developed a set of adjudicative standards that merges Top Secret and SCI requirements. These standards could be used in granting Secret-Compartmented Access clearances. Parallel standards should be established for Secret clearances.

Implementation of standards for adjudicating background investigations can eliminate multiple readjudications. For example, the Commission found that the Defense Industrial Security Program sometimes grants clearances on the basis of precedent or case law amassed through years of appeal hearings. In some cases, adjudicative decisions appear to deviate substantially from adjudicative norms followed by other organizations in the DoD. As a result of a few decisions, various special access programs and Federal agencies have developed a wholesale distrust of the industrial clearance process, leading them to readjudicate industrial security clearances. The establishment and enforcement of a single adjudicative standard would eliminate the need for costly readjudications.

Savings would also be realized within departments and agencies that have suitability requirements not related to security which they apply in pro-

cessing candidates for employment. Such assessments could be accomplished in less time and at less cost if the requirement to also readjudicate security-relevant information is eliminated.

The Commission recommends that the Secretary of Defense and the Director of Central Intelligence develop and adopt a common set of adjudicative criteria for access to generally protected and specially protected information.

DoD Adjudicative Facilities

The DoD currently **has 18 separate adjudicative organizations** but is in the process of consolidating them into eight facilities. Staffing of the various **adjudicative centers varies widely** (one center will have a staff of one) and most are neither timely in their **actions nor responsive to their customers. Virtually all face** significant budget reductions despite the fact that several are already substantially understaffed and underequipped. Few adjudicative organizations have strategic plans for integrating their information with the customer base or employing automation to manage the process.

The **DoD community** would benefit substantially from consolidating its adjudicative operations. By building on the most successful adjudicative processes and automation models, consolidation would improve the efficiency effectiveness, and consistency of the adjudicative system Research by **PERSEREC** has clearly demonstrated that larger **adjudicative facilities tend to be** more efficient. The **direct** savings of **having** a single adjudicative facility in the DoD pale in comparison to the savings **to be realized** through increasing the **timeliness** and customer responsiveness of personnel **security** programs.

Research by PERSEREC has clearly demonstrated that larger adjudicative facilities tend to be more efficient.

The Commission believes that the NSA should be excluded from the **consolidation of adjudications in the DoD.** At the **NSA, the clearance process is inextricably linked to the hiring process** much as it is for the **CIA.** The Commission believes that it could be counterproductive to integrate such employment-related adjudications into the central adjudication facility.

The Commission recommends that all DoD adjudicative entities, except the NSA, be merged into one organization reporting to the appropriate Under Secretary or Assistant Secretary of Defense.

Reciprocity

The Commission examined the practice of numerous program managers, particularly those within SAPs, exercising their option to readjudicate already cleared individuals. This adjudication is ostensibly for "access" authorization and not for clearance, but the process is virtually the same and may be repeated over and over again depending on the number of programs involved.

Recently, 149 engineers at *a* major *defense* contractor *were all cleared for SCI to work on an existing contract. After the contract was completed, these same engineers were badly needed for another SCI contract in the same facility and complex. However, it took months for the engineers to be re-adjudicated and approved for the second SCI program.*

The Commission is not convinced that such readjudications provide additional security benefits and is concerned about the significant costs resulting from the delays that such readjudications impose upon the system. The Commission believes that if SAP and other special program managers truly have personnel security requirements that are not being addressed in the clearance process, they should take action to insure their requirements become incorporated into current and future adjudicative standards. Beyond that, validation of an existing clearance should be all that is required to give an individual access to information once it has been determined that the individual has a need to know the information.

The Commission *is not convinced that such readjudica tions provide additional security benefits and is concerned about the significant costs resulting from* the *delays that such readjudications impose.*

The Commission recommends that:
a) Any individual who has an existing clearance not be readjudicated.
b) Program managers be limited to the following prerogatives when making access determinations:
1) Verifying that the individual has the requisite clearance.
2) Verifying that the individual has a need to know the classified information.

Virtually all agencies employ risk management to grant exceptions to the adjudicative standards for high risk/high gain individuals. This takes into account operational needs, unusual expertise, or other factors. However, few record these exceptions in shared information systems. Any conditional clearance or waiver of normal adjudicative criteria should be readily identifiable to other organizations that may subsequently employ the individual. This will be facilitated by implementation of central clearance verification as recommended below.

The Commission recommends that agencies identify conditional clearances or waivers through use of the standard codes in a new central data base.

PROCEDURAL SAFEGUARDS

In this section of its report, the Commission will deal with certain procedural protections and administrative remedies that may or may not be available when security clearances are denied or revoked.

In order to give its considerations some focus and manageable limits, the Commission has elected to deal only with those questions to which its partic-

ular attention was called by the Conference Report that accompanied the Defense Authorization Act For 1994. Section 1183 of that Act directed the Secretary of Defense to "conduct a review of the procedural safeguards available to Department of Defense civilian employees who are facing denial or revocation of security clearances," and further directed that this review, the results of which are to be reported to the Congress by not later than March 1, 1994, should specifically consider the following:

(A) "Whether the procedural rights provided to Department of Defense civilian employees should be enhanced to include the procedural rights available to Department of Defense contractor employees."

(B) "Whether the procedural rights provided to Department of Defense civilian employees should be enhanced to include the procedural rights available to similarly situated employees in those government agencies that provide greater rights than the Department of Defense."

(C) "Whether there should be a difference between the rights provided to both Department of Defense civilian and contractor employees with respect to security clearances and the rights provided with respect to sensitive compartmented information and special access programs."

These questions were **further** elaborated by the Conference Report, as follows:

> The conferees direct the Secretary to ensure that the review specifically address each of the following procedural safeguards in the context of the denial or revocation of security clearances with respect to civilian employees of the Department of Defense: (1) notice of the reasons for the proposed denial or revocation; (2) an opportunity to respond; (3) the right to a hearing or other appearance before a tribunal; (4) the right to be represented by counsel; (5) the availability of trial-type procedures, such as the opportunity to present and cross-examine witnesses; and (6) the opportunity to appeal any final decision. If the Secretary determines that DoD civilian employees should not be provided with procedural rights that are as protective as those afforded to DoD contractor employees with respect to any of the foregoing matters, the Secretary's rationale for each such difference should be set forth in the report.

The Conference Report then added this comment:

> The conferees note that the subject of security clearances within the Department of Defense is undergoing detailed review by the Joint Security Commission established by the Secretary of Defense and the Director of Central Intelligence, which is scheduled to complete its work by February 1, 1994. The conferees agree that the Secretary should obtain the views of the Commission on the issues set forth in the conference agreement, but note that the final responsibility for addressing these issues and issuing an implementing regulations rests with the Secretary.

The Commission has adopted this comment as its framework. because both the broader questions posed by the Act, and the more exact questions posed by the Conference Report, take as their baseline the procedural safe guards available to DoD contractor employees, some preliminary discussion

is necessary in order to understand that baseline. It is also necessary to understand how the procedures and remedies that lie along that baseline compare with the safeguards that are available to civilian DoD employees, and with the different safeguards that apply when special access approvals are denied or revoked on security grounds other than need-to-know grounds.

DoD Contractor Personnel

Background investigations relating to DoD contractor personnel are conducted by the Defense Investigative Service. If an investigation develops information that must be adjudicated in order to determine if a security clearance should be denied or revoked, the case is referred to the Directorate for Industrial Security Clearance Review (DISCR), which conducts the adjudicative process, as it also does in cases involving contractor personnel doing classified work for some 20 other government agencies or organizations, not however including the CIA, or the NSA. The adjudicative process is authorized and directed by EO 10865 (1960), as amended by EO 10909 (1961), and an implementing regulation, DoD Directive 5220.6. The Director of DISCR reports to the Deputy General Counsel of the DoD.

The government has an initial burden to show that the allegations in the Statement of Reasons have some substantial support, but the ultimate burden . . . falls on the other side.

Thousands of cases are referred to the DISCR each year. If in any case the DISCR is able to make the requisite finding of clear consistency with the national interest, based on the criteria set forth in Directive 5220.6, that finding resolves the case and the clearance is granted. Otherwise the DISCR prepares a Statement of Reasons which resembles a civil complaint and must state in detail (so far as national security considerations permit) the reasons why it may not be clearly consistent with the national interest to grant or continue a clearance. The Statement of Reasons must be provided to any person to whom it relates. Such persons also are informed that they are obliged to answer every allegation in the Statement of Reasons within 20 days, that they have a right to a hearing before an Administrative Judge, that the government will be represented by counsel at that hearing, and that they may also be represented by an attorney of their own choice and at their own expense. There is no provision for the assignment of defense counsel at public expense.

If the hearing right is exercised, there is some opportunity for discovery, essentially limited to proposed exhibits and non-privileged documents in the control of the DISCR. Testimony at the hearing is taken under an admonition by the Administrative Judge that the Federal false statement statute, which carries criminal penalties, is applicable to that testimony. Witnesses are subject to cross-examination, except that under some circumstances, again for reasons of national security, the right of cross-examination may be curtailed or denied. Although witnesses may be requested to appear or instructed by their agencies or employers to appear, and are paid per diem and travel expenses if they do so, neither government counsel nor the defense has the power to compel the attendance of witnesses by subpoena. The government has an initial burden to show that the allegations in the Statement of Reasons have some substantial support, but the ultimate burden--on the issue of clear consistency with the national interest-falls on the other side. Defense evidence may be submitted not only in rebuttal, but also in mitigation or extenuation. The Federal Rules of Evidence are used as a guide. The Administrative Judge renders a written decision, which may be appealed by the losing party to a three-member Appeal Board, which reviews the record and rules on alleged

errors. The Administrative Judge and the members of the Appeal Board are attorneys and are part of the DISCR organization.

If no hearing is requested, the case is decided by an Administrative Judge on the written record, including the Statement of Reasons, documents that provide the basis for the allegations in the Statement of Reasons, any answer or objections to the Statement of Reasons, and any other material submitted in rebuttal, mitigation or extenuation. Decisions made on such a record are also reviewable by the Appeal Board.

DoD Civilian Personnel

The procedural safeguards and administrative remedies available to DoD civilian personnel, and to military personnel as well, are prescribed by another DoD regulation, namely 5200.2-R. This regulation provides that no final adverse action can be taken, in any matter involving a personnel security determination, unless the person concerned has been given: (1) a written statement of the reasons for the proposed action, as specific and detailed as Privacy Act and national security considerations permit; (2) an opportunity to respond in writing to that statement, to whatever authority the head of that person's component within the DoD may designate; (3) a written decision by an identified official, within 60 or at most 90 days thereafter, again stating reasons as specific as Privacy Act and national security considerations permit; and (4) an opportunity to appeal to a higher authority designated by the person's component within the DoD.

There are . . . policy issues raised by the differences between the sets of safeguards.

The opportunity to submit a written response, although the regulation is not explicit on the point, implicitly includes the chance to submit any materials in support of such a response, whether in order to rebut the factual allegations or to explain any mitigating or extenuating circumstances. Likewise, although the regulation does not explicitly refer to representation by counsel, as a practical matter any person desiring to retain counsel at his or her own expense could hardly be prevented from doing so.

The regulation also reserves to the Secretary of Defense the authority to bypass the prescribed procedures and to find that a person is ineligible for a clearance, if national security interests so require. That authority may not be delegated by the Secretary, and so far as the Commission knows, it has never been invoked. A similar proviso is contained in the directive applicable to contractor personnel, but again as far as the Commission knows, it too has never been invoked.

The regulation, in an appendix, sets forth the same adjudicative criteria as the directive applicable to DoD contractor personnel.

Differences and Comparative Advantages

It is not the role of the Commission to attempt to pass judgment on the legal sufficiency of any of these procedural safeguards or remedies. If any of them is legally defective, either on its face or as it might be applied in any particular case, an appropriate plaintiff will presumably come forward and any claims will then be duly determined by the courts, with the benefit of adversary briefs and on the basis of a properly developed factual record.

'There are, however, policy issues raised by the differences between the sets of safeguards available to DoD contractor employees on the one hand and DoD civilian employees on the other. As the Commission sees it, the most fundamental differences are the following: contractor personnel have the assurance that they will have a chance to review all documents on which a decision is based, whereas civilian employees, although in practice they may be provided with such materials, appear to have no such assurance; contractor personnel, unlike civilian personnel, have a right to a trial-type hearing, at which the government has an initial burden of showing that its allegations. have some substantial support, at which witnesses testify subject to cross-examination, and at which the Federal Rules of Evidence are used in at least a guideline sense; and more generally, the cases involving contractor personnel, assuming the hearing right is exercised, are handled in a more formal manner, akin to judicial proceedings, with the government's side represented by a qualified trial attorney and with the final decision in the hands of an Administrative Judge who is also an attorney, and a three-member Appeal Board also composed of attorneys.

It is the premise of the questions posed in the Conference Report to which we have already alluded, and it is also the position of the American Bar Association, which has been outspoken on the matter, that the procedural safeguards available to DoD contractor personnel are superior to the safeguards to which DoD civilian personnel are entitled. However, it is not at all self-evident that this is so.

To begin with, as nearly as the Commission can tell, the right of a contractor employee to demand a trial-type hearing before an Administrative Judge is made absolute by the applicable directive, whether or not there are any factual disputes that need to be resolved. Not even civil litigants operating under the Federal Rules of Civil Procedure have as broad a right. On the contrary, those rules effectively foreclose any opportunity for a trial in any case in which the material facts are undisputed, and the only genuine issues concern the significance of those facts. In addition, contractor employees are evidently free to demand a trial-type hearing not only in circumstances where they do not contest the government's allegations and do not have any rebuttal evidence, but also where they desire only to present some information that may be extenuating or mitigating. Even assuming that such a broad hearing right may be superior from an employee's standpoint, and may be available in other contexts involving for example the denial or revocation of professional licenses, that does not mean that such a right is required in the name of fundamental fairness, or that is should become the universal standard in connection with decisions that are as highly discretionary and judgmental as clearance decisions.

Second, while it is true that contractor employees have the right to be rep resented by counsel at their own expense, that right is empty for those who cannot afford that expense or obtain pro bono representation. Such persons are left with the prospect of facing an experienced trial attorney alone and without representation. Civilian employees may also go unrepresented, but they are not caught up in a system in which there is an experienced trial attorney on the government side. Further, even where contractor employees are able to avail themselves of the right to counsel, that may be only because their employers agree to bear the expense, which is not a possibility in cases involving civilian DoD employees. In our estimation, although we haven't seen any

evidence on the point, there is a somewhat lower chance that an employee union might come forward to pick up the expense of such employees.

Third, in contractor employee cases, the employee's right of appeal from an adverse decision is confined by strict scope-of-review limits. The Appeal Board may not consider any evidence not considered by the Administrative Judge. Nor is the Appeal Board free to reverse a decision except on grounds that it was arbitrary, capricious, or contrary to law, or that the factual findings were unreasonable, or that procedural error was committed. These same constraints do not exist in civilian employee cases. The appeal authorities in those cases can take an entirely fresh look and make what they believe to be the appropriate decision, without regard for the lower-level decision, which is apt to be far less detailed than a decision of an Administrative Judge in the DISCR process. Further, while either losing party, which may be the government, can appeal the decision of an Administrative Judge, in civilian employee cases there does not appear to be any provision for appeals of decisions that are favorable to the employee.

Fourth, the system of adjudicating contractor employee cases has a rigidity that can work against the employee. No allowance is made in that system for the value that such employees may bring to the classified work being performed by their employers. No matter how high that value, it does not figure in the adjudicative criteria, and it is therefore ignored. The civilian employee system, however, is flexible enough to take account of that value. In that system, either at the lower level or the appeal stage, decisions can be influenced by arguments that the employee is a big contributor, that any security risk is manageable, and therefore that the risk should be taken. There is also a good chance that supervisors within an employee's component will actually come forward to champion such arguments or to make other arguments on the employee's behalf.

The system of adjudicating con tractor employee cases has a rigidity that can work against the employee.

We do not say any of this to denigrate in any way the DISCR process. Rather we make these points only to show that the policy debate is not one-sided, and because it is very unclear to us whether, given a choice between the DISCR process and the existing arrangements, civilian DoD employees would opt for the former. It is even more unclear to us that military personnel, who have an understandable confidence in their own chain of command, would opt for the DISCR process.

We come now to the specific questions posed by the Conference Report, which were directed to the Secretary of Defense but as to which the views of the Commission were invited. These questions asked why, in each of six different respects, "DoD civilian employees should not be provided with procedural rights (in connection with the denial or revocation of a security clearance) that are as protective as those provided to DoD contractor employees."

1. Notice of the reasons for the proposed denial or revocation. In this respect, as the Commission understands, any difference between the rights afforded to the two classes of employees is a matter of degree. The Statement of Reasons that commences the DISCR process is apt to be a more detailed statement than the notice provided to civilian employees. Without attempting to draw any fine lines, the operative principle here should be that affected employees are entitled to a statement that adequately informs them of the fac-

tual basis of any proposed adverse action, and that identifies the adjudicative criteria that are relevant under the circumstances.

2 An opportunity to respond. Here again the Commission believes that this opportunity is already afforded to both classes of employees. In any event, the Commission believes that it should be.

3. The right to a hearing or other **appearance before a tribunal. A** hearing and a trial-type hearing are not synonymous terms. Many forms of proceedings, including some more informal than those now available to civilian. DoD employees, could accurately be described as hearings, even though they don't have the characteristics typically associated with trials, such as live testimony subject to cross-examination and precise rules governing the admissibility of evidence. The real issue here is not whether there should be a right to some sort of hearing, because civilian DoD employees already have that right. The issue is whether the hearing rights of civilian employees and contractor employees should be conformed, which is an issue we discuss in a moment, under the caption "The availability of trial-type procedures."

The issue is whether the hearing rights of civilian employees and contractor employees should be conformed.

So far as concerns the right to an "appearance before a tribunal," the Commission understands that as matters stand today, civilian DoD employees cannot demand, with any assurance that the demand will be granted, an opportunity to appear personally before any designated adjudicative authority that is considering whether to deny or revoke a clearance. The Commission believes such an opportunity should exist.

4. The right to be represented by counsel. This right exists today, although it is diluted by the fact that employees who retain counsel must do so at their own expense, and the cost may be beyond the means of many employees. We note again that contractor employees, particularly senior officials, may have an important edge here, because for them, unlike civilian DoD employees, there is at least a possibility that the employer may agree to bear the cost of any legal representation. The Commission also believes that while the right to counsel is secured to civilian employees in the sense that there is nothing to stop them from consulting an attorney if they choose to do so, such employees should be explicitly informed, as are contractor employees, that they have this right.

5. The availability of trial-type procedures, such as the opportunity to present and cross-examine witnesses. The availability of such procedures to DoD contractor employees, and their unavailability to DoD civilian employees, is the most dramatic difference between the two adjudicative systems. The hard question posed by the Conference Report is whether such procedures should be extended to the civilian employees.

The Commission recognizes that there may be complex legal issues that come into play here, and that the nature of those issues may vary from one individual case to another, depending for example on such circumstances as whether the person affected is an initial applicant for a clearance or already holds a clearance, whether the denial or loss of a clearance leads to the loss of a job, and whether and if so how far and in what way the person's reputation may be impaired or the person may otherwise be stigmatized by an adverse decision. Again, however, any legal issues are for courts to determine, and are beyond the purview of the Commission.

On balance, ***from*** solely a policy standpoint, the Commission does not favor the idea of extending trial-type procedural protections to civilian DoD employees.

As already noted, the hearing rights currently granted to contractor employees are broader and more absolute in important respects than even the hearing rights available to civil litigants whose claims and defenses are adjudicated in the Federal courts. No matter what interests such litigants may have at stake, they are not entitled to a trial, and their claims or defenses may be resolved against them on the basis of written submissions, unless they are able to show that there is something to have a trial about-namely, a **material** factual dispute that needs to be resolved. Contractor employees faced with a denial or loss of a clearance, however, are evidently entitled to a trial-type hearing, on demand, without making such a showing.

The extension of such a broad hearing right to civilian employees could well result in a great many trial-type hearings in cases involving only undisputed facts. It would certainly have the result of putting a great many more discretionary clearance decisions into the hands of judges. It would also introduce new and significant delays into the system, because it is unquestionably the fact that cases handled under the DISCR process, if trial-type hearings are demanded, on the average take far longer to resolve than cases adjudicated on a written record. Such delays are not merely a matter of inconvenience. One practical effect is that persons who are applicants for an initial clearance, and have been assigned to positions requiring a clearance, cannot move into those positions so long as the clearance outcome remains in doubt. Other difficulties arise if a person already holds a clearance that is threatened with revocation. If that clearance is a job requirement and is suspended pending the outcome of the revocation proceedings, the person cannot perform the job in the meantime. If the clearance is not suspended pending the outcome, a security risk must be taken in the meantime. In all these circumstances there is a price to be paid, not just by the employee but also by the government.

To be sure, there will always be cases that do involve serious factual disputes, and in which the existence or non-existence of those facts and the credibility of witnesses might be determined with more certainty if trial-type procedures were employed. There may also be cases in which an experienced Administrative Judge might be better able to apply the clearance criteria even to undisputed facts than other adjudicators. These considerations, however, do not persuade the Commission to alter its policy advice. Trial-type **procedures** are at their most effective in promoting fairness and accuracy only when both sides are equally represented. In the DISCR process only the government is sure to be represented. The same would be true if the DISCR model was followed for DoD civilian employees. The Commission is also influenced in its view by the fact that such employees are less likely than contractor employees to lose their jobs, or to incur serious damage to their careers, if a clearance is denied or revoked. And the Commission is also influenced by its doubt that, if given the choice, most civilian employees would prefer the DISCR process to the system now in place.

At the same time, the Commission believes that the fairness of the **system** now in place can and should be improved. In particular, the procedural protections now available to DoD civilian employees should be expanded to include the same explicit right to review any documents on which a proposed denial or revocation of a clearance may be based, or which are germane to

The Commission believes that the fairness of the system now in place can and should be improved.

such a proposed action, that is presently afforded to DoD contractor employees. This opportunity should be afforded as early in the process as possible, so as to make it useful to the employee in preparing an initial written response to the allegations set forth in statement of reasons that commences the process.

6. The opportunity to appeal any final decision. This right exists today. Indeed in some ways, as already noted, the appeal available to civilian employees may be a more valuable right than the appeal available to contractor employees, because the latter is constrained by scope-of-review limits whereas the former gives the employee a true "second bite at the apple." Nevertheless, the Commission realizes that the appeal procedures vary from one DoD component to another and believes that these procedures should be standardized and should provide for review by appeal boards consisting of three members. In the Commission's view these boards should have a diverse membership, including at least one senior official in the employee's DoD component and, in the absence of an attorney adviser to the board, one **attorney. Part** of the **purpose here would be** to **ensure** a **broad** perspective, and a review that is not solely in the hands of security officials.

The Commission recommends that:

a) The DISCR process, with its trial-type procedures, not **be adopted as the model for the adjudication of security clearance cases involving DoD civilian employees.**

b) All DoD civilian employees facing the possible denial or revocation of a security clearance be explicitly informed that they have a right to counsel.

cl Any documents on which a proposed denial or revocation of a security clearance is based, or which are germane to such a proposed action, be made available for timely review by the affected DoD civilian employee, so far as applicable privileges and national security considerations permit.

d) Any DoD civilian employee be given the opportunity to appear personally before any adjudicative authority that is considering whether to deny a clearance to such an employee, or to revoke a clearance held by such employee.

e) Any DoD civilian employee have a right to appeal any adverse clearance decision to an appeal board consisting of three members, one of whom should be a senior official in the employee's DoD component and another of whom, unless the board has an attorney, should be an attorney.[13]

Military Personnel

Even though issues relating to military personnel are outside the bounds of the recent congressional inquiries that the Commission took as its framework, the Commission has considered whether there is any good reason why DoD military personnel should be treated any differently than DoD civilian personnel in regard to the denial or revocation of security clearances. In the Commission's view there is no such reason, and it is bolstered in that view by

the fact that the DoD regulation applicable to civilian personnel, 5200-2-R, is similarly applicable to military personnel.

The Commission recommends that, so far as concerns the denial or revocation of security clearances, DoD military personnel be afforded all the same rights as DoD civilian personnel.

Special Access Approvals

The Commission now turns its attention to another question posed by the Congress in the 1994 Defense Authorization Act, which was "whether there should be a difference between the rights provided to both Department of Defense civilian and contractor employees with respect to security clearances and the rights provided with respect to sensitive compartmented information and special access programs."

This question arises because DoD Directive 5220.6, which is the regulation applicable to the denial or revocation of contractor employee clearances, explicitly provides that it "does not apply to cases for access to sensitive compartmented information or a special access program"; because DoD 5200.2-R, which is the regulation applicable to the denial or revocation of civilian employee clearances, may or may not be followed in connection with the denial or revocation of access to a SAP; and because denials or revocations of access to Sensitive Compartmented Information (SCI) is governed by DCID 1/14, issued under the authority of the Director of Central Intelligence, which establishes yet another set of procedures.

These different procedures owe their existence to the fact that special access and SCI security determinations have historically involved the application of more selective and stringent adjudicative criteria than clearance determinations. If the Commission's basic classification system recommendations, and its recommendation that there be a common set of adjudicative criteria, are adopted, the rationale for these different procedures would disappear. There would no longer be any separate special access determinations, except on need-to-know grounds. The clearance decisions would then settle the matter of eligibility for all purposes, either at the Secret level or at the Secret Compartmented Access level. The denial or revocation of clearances in DoD contractor personnel cases would be subject to the DISCR process, and the Commission believes that DoD civilian employee cases should then be subject to existing DoD procedures (the 5200.R-2 procedures), as modified by the Commission's recommendations in this section of its report.

If on the other hand the Commission's classification system and adjudicative criteria recommendations are not adopted, with the result that SAP and SCI access determinations continue to be based on separate and more demanding requirements than clearance determinations, then further judgments will need to be made about the procedural safeguards that should apply to the denial and revocation of an access approval. In that event, the Commission believes that the appropriate safeguards for both DoD civilian and contractor employees are those prescribed by DoD 5200.2-R, again as modified by the recommendations in this section of the report. The Commission does not recommend that the denial or revocation of an access approval,

There would no longer be any separate special access determinations, except on need-to-know grounds.

if such an approval remains distinct from a clearance decision, be made subject to the DISCR process, even as to DoD contractor employees.

THE POLYGRAPH

The polygraph is a controversial investigative technique. While some argue that the polygraph is the most effective information gathering procedure available, others point to its lack of scientifically established validity, the overreliance on passing polygraph examinations as a "guarantee" of trustworthiness, and the belief that it is unacceptably intrusive and violates personal privacy. The Commission was asked to undertake an objective review of the Federal personnel security screening polygraph program to determine how well it works, how it could be improved, and whether it should be continued.[14]

Background

The polygraph[15] is a multichannel instrument that records changes in respiration, cardiovascular activity, and skin resistance in response to questions. According to polygraph theory, when a subject gives a false response to a relevant question (questions of concern to security adjudicators), the physiological reaction will be greater than the reaction to other questions (control or irrelevant questions). However, contrary to popular belief, there is no physiological response that is unique to deception. The reactions measured by the polygraph can be caused by a variety of emotions. This fact underlies much of the controversy surrounding the polygraph.

The polygraph process consists of a pretest interview, test phase, and posttest interview. During the pretest interview the polygraph examiner tries to establish rapport with the subject, reviews with the subject the background history statement, familiarizes the subject with the polygraph instrument if necessary, and then enters into a detailed explanation and discussion of the exact questions that will be asked during the test phase of the exam. It is generally not explained to the subject that there will be two or more different types of questions asked during the examination. There are questions of primary interest such as "Are you engaged in espionage?" or "Within the last 5 years have you used, possessed or sold any narcotics or dangerous drugs?" These questions are also known as "relevant" questions. Also included are a series of questions designed to assist the examiner in calibrating the subject's responses to the relevant questions during the test phase. Depending upon the polygraph technique used, such a question may be an irrelevant question (Are you wearing shoes?) or some type of a control question (Have you ever betrayed the trust of someone who depended on you?). The subject may or may not be asked to lie in response to the control questions and at present, most subjects are not told to lie. The examiner, who is a trained investigator and usually highly skilled in interrogation, will encourage the subject to "come clean" on each of the relevant questions while at the same time attempting to restrict or minimize the subject's answers to the control questions.

Significant admissions to relevant issues are explored fully through interrogation. Unimportant admissions are excluded by modifying the questions.

Significant admissions to relevant issues are explored fully through interrogation. Unimportant admissions are excluded by modifying the questions

with, "Except for what you have disclosed to me, have you ever . . . ?" This process continues until the subject is able to answer all questions with a "yes" or "no" and the examiner is convinced the subject will properly respond to all types of questions posed during the exam, that is, a guilty subject will react to the relevant questions while an innocent subject will react most significantly to the control questions.

During the test phase the subject is attached to the polygraph instrument and is limited to responding "yes" or "no" to the relevant and control questions asked. The test phase is generally very short in duration. During the posttest phase, the subject is given an opportunity to explain any reaction to certain questions. Standard interrogation techniques are employed, but only responses to relevant questions are explored with the subject. If the subject offers an admission, the test is readministered with the question causing the reaction changed to "Other than what you have told me, . . . ?" or a new set of questions are asked that focus more narrowly upon the issue(s) in question. This process continues until the subject no longer reacts to any of the (modified) relevant questions, the subject terminates the interview, or the examiner determines that additional testing may need to be conducted at a later time.

Establishing the proper examination setting is challenging for the examiner and can be very stressful to both innocent and guilty subjects. Even innocent subjects have to undergo an extremely unpleasant self-examination, before a government investigator, regarding highly personal information, while knowing that the whole proceeding is being recorded. Many Commissioners were troubled by the wide latitude given to examiners and the possibilities for abuse, especially where relevant and control questions are used to elicit highly personal information of questionable relevancy to security screening. While attempts can be made to minimize the discomfort level for innocent subjects such settings can and do result in anguish and in complaints of abuse.

Establishing the proper examination setting is challenging for the examiner and can be very stressful to both innocent and guilty subjects.

Applications of the Polygraph

The DoD and the Intelligence Community use the polygraph in the following areas: specific issue investigations (criminal and security), personnel security screening, and operations (vetting and validation of intelligence sources). The Commission evaluated the use of the polygraph in personnel security screening only. Specific issue investigations and operational uses of polygraph were outside the scope of this review.

Two types of polygraph examinations are currently used in personnel security screening: the counterintelligence-scope (CI-scope) polygraph and the full-scope polygraph. The CI-scope polygraph focuses on espionage, sabotage, terrorism, subversion, mishandling of classified information, and unauthorized contacts with representatives of foreign governments. The full-scope polygraph covers all of the CI-scope questions and a number of issues that pertain to both security and suitability for employment (questions that have been inaccurately labeled "lifestyle"). These questions may address any of the following issues: criminal history, serious financial problems, use of illegal drugs, excessive use of alcohol, falsification of information on the personal history statement, and serious nervous or mental disorders. Questions about sexual orientation are no longer asked during polygraphs. The entire polygraph process (pretest, test and posttest) in the DoD and the Intelligence

Community is recorded (video and/or audio). The recording is justified on quality control grounds, but it also raises concern because it creates a record of extremely sensitive, personal information about the applicant.

Screening polygraphs, particularly the full-scope polygraphs, are more controversial than specific issue polygraphs because they cover a wider range of personal matters and are administered to individuals who are not suspected of specific wrongdoing. Polygraph opponents argue that screening polygraphs are intrusive dragnets for information and that individual privacy interests outweigh the government's need for such wide-ranging searches. Proponents contend that screening polygraphs are used only to seek information that is relevant to trustworthiness and therefore to national security interests. They point out that these same issues are addressed in personal history statements, personal interviews, and background investigations and that the basis for asking them derives from approved adjudicative criteria.

While senior officials at the CIA and the NSA acknowledge the controversial nature of the polygraph process, they also sf rongly endorse it as the most effective information gathering technique available in their personnel security systems.

The CIA and the NSA are the only agencies that use full-scope polygraphs to screen applicants for employment. For these agencies, the screening polygraph serves both security and suitability functions. They require the polygraph as a condition of employment because any employee of these agencies may have access to a broad range of classified information in the course of his or her regular duties. The DoD, which uses a U-scope polygraph only, has been limited by Congress to 5,000 screening polygraphs per year (with major exceptions such as the NSA, the NRO, and cryptographers). The DoD's use of the screening polygraph is not related to employment. Rather, these polygraphs are administered to people who already occupy sensitive positions but require access to a specific or several sensitive programs for which the polygraph has been established as a requirement.

The following arguments have been made in favor of the polygraph:

a. ***A Unique Source of Information: Officials*** at the CIA and the NSA point out that the polygraph elicits important adjudicative information that is often not obtainable by other investigative methods, such as personal history statements, personal interviews, and background investigations. In fact, the most important product of the polygraph process is more likely to be an admission made during the interview than a chart interpretation. While senior officials at the CIA and the NSA acknowledge the controversial nature of the polygraph process, they also strongly endorse it as the most effective information gathering technique available in their personnel security systems. They argue that without the polygraph, the quality of their work force would suffer immeasurably.

The DoD uses a U-scope polygraph only after individuals have been thoroughly investigated and favorably adjudicated. Nonetheless, DoD officials report that they have obtained significant security and counterintelligence admissions that were not developed through the prescreening and investigative process. The DoD catalogues and reports these results annually to Congress.

The utility of the polygraph in eliciting important adjudicative information is not in doubt. In addition, the Commission found that the suitability or "lifestyle" questions (particularly those that address criminal activity and illegal drug use) have always elicited the most information. Research studies have supported these views:

- In 1980 a working group of the DCI Security Committee found that the polygraph examination process was superior to other investigative methods in eliciting adverse information that ultimately resulted in denial or revocation of access.

- An April 1991 study by the Personnel Security Working Group, (an Intelligence Community interagency working group), unequivocally identified the polygraph as the most productive source of derogatory information in the screening arena, eliciting such information in 70 percent of the cases in which it is used.

- A September 1993 CIA study cited the following polygraph benefits: it enables the CIA to forgo random drug testing for staff employees or those with staff-like access; it facilitates the flow of classified information within the organization; it enables the CIA to use minimal internal information systems security checks; and it reduces the need for domestic physical security countermeasures.

b. *Deterrence:* Screening polygraph programs arguably have a deterrent effect. Applicants who believe that the polygraph will elicit disqualifying information may be deterred from applying. Cleared personnel also may be deterred from misconduct because they know that they will be required to take a polygraph in the future. In fact, the CIA's Inspector General noted that the polygraph has been instrumental in reducing the incidence of fraud and other wrongdoing at the CIA. In addition, a 1993 study by the DCI's Counterintelligence Center and an Intelligence Community research project have concluded that the polygraph is a significant espionage deterrent.

c. *Cost-Effectiveness:* The CIA and the NSA, two agencies that routinely use full-scope polygraphs to screen applicants, present a strong case that the polygraph serves as an efficient and effective cost-containment hiring tool. When admissions made by a subject during a polygraph test result in a disqualification, these agencies are saved the considerable cost and time of conducting a background investigation. In addition, the CIA's Office of Medical Services reported to the Commission that full-scope polygraphs enable it to detect and screen out 50 percent to 75 percent of the most troubled applicants. They expressed concern that if the suitability questions were reduced or eliminated this would result in increased terminations for cause, security breaches, and medical, legal, and administrative costs arising from contested terminations and increased psychiatric difficulties in the work force.

The polygraph is a significant espionage deterrent.

The following arguments have been made against the polygraph:

a. ***Lack of Scientific Validity: In 1983, the*** Congressional Office of Technological Assessments concluded that: "There appears, as yet, to be no scientific field evidence that polygraph examinations . . . represent a valid test to prescreen or periodically screen government employees." A 1991 government review of the polygraph in personnel security applications reaffirmed the earlier study and concluded that "the number and quality of screening studies is insufficient to provide a basis for reliable estimates of validity." The Commission reviewed many other studies as well. The results of these studies were too varied to allow for definitive conclusions about the validity of the polygraph when used for personnel security screening. The Commission also met with various research experts in polygraph and related fields and learned that

due to the extraordinary difficulty of conducting screening polygraph validity research, the scientific validity of the polygraph is yet to be established.

Many polygraph proponents and some research experts believe that it is unnecessary to study the validity of the polygraph process, meaning its accuracy in distinguishing truth from deception. They contend that as long as the polygraph elicits admissions to screen out unsuitable applicants and actual security risks, questions about the polygraphs validity remain academic. However, if the polygraph does not have established scientific validity in the screening arena, judgments about truthfulness based solely on chart interpretation will continue to be controversial. Without established validity, the process lacks full integrity and appears more like trickery because information is obtained from subjects under the pretense that it is in their best interest to be forthright since false answers will be discovered. Furthermore, arguments could be made that the polygraph may not have the same effect on a nonbeliever; that is, unless the validity of the process can be demonstrated, there is nothing to prevent a practiced deceiver from passing a polygraph examination. In fact, circumstantial evidence lending credence to this view was documented by a President's Foreign Intelligence Advisory Board study in 1988.

Comparison or control questions are frequently identified as the most intrusive aspect of the polygraph.

b. *Intrusiveness:* Polygraph testing can be a highly intrusive and emotionally grueling process. Some claim that this results in lost talent when suitable individuals refuse to participate in a polygraph examination. Other individuals and organizations have argued that there can be no justification for the use of the polygraph. The Department of State has refused to use the polygraph for personnel security screening, even for those with access to the most highly protected information. The ACLU views the polygraph as an unacceptable invasion of privacy, an affront to human dignity, a violation of self-incrimination prohibitions, and an unreasonable search and seizure.

Comparison or control questions are frequently identified as the most intrusive aspect of the polygraph. Control questions are used to elicit untruthful or uncertain responses from subjects (for example, "Have you ever violated the trust of a close friend?"). Physiological reactions to these questions are compared to reactions to the relevant questions (for example, "Have you ever committed a serious crime?"). It is assumed that "innocent" subjects will react more strongly to the control questions than the relevant questions, while the reverse will be true for "guilty" subjects. For this reason, "innocent" subjects frequently experience the control questions as intrusive or embarrassing (indeed, the intent is to generate some degree of discomfort) and worry that their responses will be kept in a permanent record.

The DoD has developed a less intrusive type of control question called the directed lie. In this technique, the examiner directs the subject to lie in response to certain questions (the control questions) so that a physiological reaction can be obtained while lying. Directed lie control questions differ from other types of control questions in that the subject is specifically instructed to lie to these questions and no admissions are solicited or allowed. Knowing their true purpose, people generally experience these questions as less intrusive. Research is currently under way to further validate this technique.

As unpleasant as the polygraph process may be to some individuals, the Commission did not find any ground swell of antipolygraph feeling among the government and contractor personnel who are most heavily exposed to it. On the contrary, available surveys suggest the majority of those who take a

screening polygraph believe **that the examinations are conducted fairly and** professionally.

c. *Over reliance:* In the absence of admissions, polygraph tests are not infallible: truthful subjects sometimes "fail" and untruthful subjects sometimes "pass." When the polygraph test result is used as a primary determinant of "truth," there will be occasions in which innocent people are falsely accused and guilty people avoid detection.

In the absence of admissions, polygraph tests are not infallible.

Despite assertions to the contrary, adjudicative decisions have been made on the basis of polygraph chart interpretations without admissions. Managers and security officers who make decisions based on polygraph test results need to be aware of the fallibility of the polygraph screening process. Also, the Commission is concerned that, in times of declining financial resources, agencies may be tempted to rely more on the polygraph at the expense of more thorough investigations, decreasing the checks and balances provided to the personnel security process by background investigations and financial checks and increasing the likelihood of spies being hired or allowed to continue espionage activities started after initial employment.

Recommendations

Despite the controversy, after carefully weighing the pros and cons, the Commission concludes that with appropriate standardization, increased oversight, and training to prevent abuses, the polygraph program should be retained. In the CIA and the NSA, the polygraph has evolved to become the single most important aspect of their employment and personnel security programs. Eliminating its use in these agencies would limit the effectiveness of security, personnel, and medical officers in forming their adjudicative judgments. However, the Commission unanimously endorses the adoption of procedural safeguards and oversight (discussed later in this section) to ensure that the technology is used in a reliable, consistent, and ethical manner. We support the standardization of the process to ensure basic fairness and reciprocity. We believe that the intrusiveness of the procedure should be minimized and mechanisms should be put in place to resolve ambiguous results quickly and efficiently.

The Commission believes that polygraph examinations should be limited to CI-scope for all security screening examinations, except for applicants seeking staff positions at the CIA and the NSA. Almost all of the Commissioners believe that polygraph examinations for these CIA and NSA staff applicants can be restricted without reducing security benefits. The Commission recommends that polygraphs for applicants for CIA and NSA staff positions consist of only the Cl-scope questions plus questions on serious criminal conduct and recent drug use. This ensures uniformity between the two agencies and eliminates broader questions about financial problems, alcohol use, nervous or mental disorders, and falsification of any information on the personal history statement. The record indicates that the questions about serious criminal conduct and recent drug use are much more likely than the other questions to produce information of significant value in making security and suitability decisions. These restrictions on the polygraph for CIA and NSA staff applicants will limit its intrusiveness without sacrificing its security benefits. A CI-scope polygraph should be used for all reinvestigations, even for CIA and NSA employees. One of the ten Commissioners believes that the CIA and the

NSA should be permitted to use the questions currently being asked during applicant screening polygraphs examinations, with due regard for the need to standardize the questions as soon as possible.

The Commission is concerned about overreliance on the polygraph. Under the security scheme we have proposed, the polygraph would not be a general requirement for access to classified information: a NACI plus credit will be required for access to generally protected information and an SSBI for access to specially protected information. Nor would the polygraph necessarily be a requirement for access to multiple specially protected programs, as it is today in the DoD. Instead, the polygraph should only be an option in those rare instances when the Secretary of Defense or the Director of Central Intelligence approves its use for particular controlled access activities, or if required as a condition for staff employment at the CIA or the NSA.

The Commission is concerned about over-reliance on the polygraph.

The Commission recommends that:

a) The screening polygraph should be used by those DoD and Intelligence Community organizations that currently employ it as follows:

1) Polygraph examinations should be limited to CI-scope for all security screening examinations except for initial applicants seeking staff positions at the CIA and the NSA.

2) The screening polygraph examinations of initial applicants at the CIA and the NSA should be limited to U-scope plus questions on serious criminal conduct and recent drug use.

3) A CI-scope polygraph should be used for all reinvestigations, even for the CIA and the NSA.

b) The polygraph should not serve as a bar to clearance reciprocity or the exchange of classified or sensitive information.

cl The intrusiveness of control questions must be minimized, strict oversight must be established to prevent abuses, information elicited by control questions must not be kept in a permanent record unless it relates to criminal activity, and procedures must be adopted to ensure compliance with these requirements.

d) Physiological reactions, without admissions, to questions during a polygraph examination should not be used to disqualify individuals without efforts to independently resolve the issue of concern

Oversight

The Commission is aware of the potential for abuse and the actual past abuses associated with polygraph programs. For example, in some instances examiners have pursued issues beyond the scope of the inquiry. We believe that the polygraph process must minimize intrusiveness as much as possible. This can be done by training examiners in less adversarial methods and by implementing rigorous quality control procedures. While a number of safeguards have been built into the current system (such as internal polygraph quality control procedures and Inspector General reviews), the Commission

believes that an external, independent, centralized oversight mechanism is needed to monitor the programs and manage complaints. Such a mechanism would provide a focal point for tracking and investigating reports of abuse and ensure that the polygraph programs are responsive to the concerns of polygraph subjects.

The Commission recommends that an independent, external mechanism be established by the security executive committee to investigate and track polygraph complaints. This mechanism also should monitor and oversee the polygraph programs' compliance with standards and conduct periodic satisfaction surveys of polygraph subjects.

Standardization

The Commission found that the personnel security screening polygraph program is characterized by a complicated web of inconsistent and misunderstood practices. Agencies vary as to when or if it is required, where or how it is administered, the subject areas covered, and what techniques are employed in administering the tests. For example, the Commission finds no acceptable reason why the CIA and the NSA should cover different subject areas in their full-scope polygraphs. The Commission also is concerned that the same questions are worded differently and are therefore open to differing interpretations, decreasing confidence in the objectivity of the process. The Commission believes that these differences should be minimized.

The Commission finds no acceptable reason why fhe CIA and the NSA should cover different subject areas in their full-scope polygraphs.

The Commission recommends that standards be developed to ensure consistency in the administration, application and quality control of **screening polygraphs.**

The need for standardization and consistency is also evident in the contractor world. The NSA is the only agency that requires full-scope polygraphs for all contractors prior to granting access to compartmented information. The DoD requires only a Cl-scope polygraph for their contractors, but generally grants access prior to (and sometimes without) administering a polygraph.[16] The CIA requires only U-scope for those contractors outside its facilities but full-scope polygraphs for those contractors with regular working access to its facilities and computer systems. Such inconsistent applications should be eliminated.

The Commission believes that enhanced efficiency and cost savings can be realized by establishing one organization to serve as the executive agent for conducting polygraphs on contractor personnel who do not require regular working access to government facilities. The executive agency would oversee the operation of joint polygraph facilities at strategic sites that would serve to maximize the efficient accomplishment of a maximum number of examinations. The executive agency would also coordinate the scheduling of all contractor polygraph examinations to economize on **travel** requirements.

Most importantly, an executive agency would facilitate the standardization of the CI-scope polygraph as well as the reciprocal acceptance of polygraphs throughout the DoD and the CL4 intelligence community The joint investigative service (described in chapter 7) would be a logical organization to perform this service.

The Commission recommends that:

al The CI-scope polygraph be adopted as the standard for all contractor personnel.

b) Polygraph examinations for ail contract personnel working at contractor facilities be conducted under the auspices of a single entity.

Training, Research, and Development

The single most significant variable in the polygraph process is the competency and integrity of the examiner.

Many believe that the single most significant variable in the polygraph process is the competency and integrity of the examiner. Any polygraph technique, no matter how benign, can be used in an abusive way by an improperly trained or misguided examiner. Competence is **a** primary requirement for ethical practice. For this reason, the Commission believes that it is essential for examiners to be formally trained and professionally certified under **a** single entity. Polygraph examiners also should be required to maintain professional certification through a formal continuing education program.

The Commission recommends that certification of polygraph examiners under the auspices of a single entity should be mandatory. Mandatory requirements for recertification also should be established.

Most polygraph training is conducted at the DoD Polygraph Institute (DoD/PI), although the CIA trains its own examiners and some from the **NSA. In the** interest of efficiency and consistency, the Commission believes that all government polygraph training and certification should be conducted by a single entity. Incorporating the CIA training program into the DoD Polygraph Institute would standardize and enhance the quality of polygraph training provided by the government. The DoD Polygraph Institute also should be made a national or Federal polygraph institute and, **if subject to** relocation due to base closure, consideration should be given to locating the institute closer to its customer base.

The Commission recommends that the CIA polygraph school be consolidated into the DoD Polygraph Institute to form a national polygraph institute that would conduct all training and certification of government polygraph examiners.

The Commission believes that it is imperative the government establish the validity of the polygraph for personnel security screening. In the absence of admissions, the ability of the polygraph to distinguish between truthful and deceptive reactions is critical. While the Commission recognizes the difficulty of designing and conducting validity research on the screening polygraph, the dearth of such research is not acceptable. The Commission realizes that these recommendations have been made in the past, with little effect. A greater commitment must be made to sustain funding of research to establish the validity of the polygraph in personnel security screening applications.

The Commission believes that research is also needed to determine which polygraph techniques work best in which situations and with which subjects. The ongoing development of scoring algorithms and computerization would increase the objectivity of the polygraph process and provide a basis for addressing countermeasure threats. We also believe that research should explore other methods of detecting deception that could be used in conjunction with or in place of the polygraph.

The Commission recommends a robust, interagency-coordinated and centrally funded research program[17] should be established with the DoD/PI as executive agent. The polygraph research program must concentrate on the development of valid and reliable security and applicant screening tests and standardize their use.

The Commission believes that it is imperative the government establish the validity of the polygraph for personnel security screening.

Chapter 5.

Physical, Technical, and Procedural Security

Many of our physical security policies are out of date, are not based on actual threat, conflict with each other, and have not been implemented in a uniform fashion.

The physical protection of information, assets and personnel is fundamental to any security system. Closely related to physical security are the technical security safeguards required to protect certain facilities against intelligence collection or observation and security procedures adopted to monitor and control physical access to facilities and material. Government rules for protection of classified information cover construction and storage requirements (facilities, locks, alarms, guards), technical security requirements imposed on facilities storing classified information (surveillance countermeasures, TEMPEST, audio attenuation), and procedures affecting the conduct of operations within these facilities (inspections, document control, visit certification, and badges).

The Commission's focus was primarily on the domestic environment where there is the greatest potential for cost savings, a lower level of threat, and because it lends itself more readily to uniformity than do facilities at overseas locations. Our review was limited to the protection of classified information and material. It did not include protection of weapons, munitions, or nuclear devices which are governed by separate regulations.

Recently there have been significant policy changes affecting physical security within the Intelligence Community. However, it appears that cross-program management for physical, technical, and procedural security countermeasures is not uniform. The relationships with industrial contractors vary from punitive compliance inspections to problem-solving advice and assistance. In addition, many of our physical security policies are out of date, are not based on actual threat, conflict with each other, and have not been implemented in a uniform fashion. As a result, the end user is faced with a patchwork of multiple standards, increased costs because facilities cannot be shared, and irrational situations where information classified at a lower level (Confidential and Secret) is often more stringently protected than our government's most sensitive technologies and operations. The wide variety of physical, technical and procedural security requirements imposed on industry is the principal concern that lead to the development of the National Industrial Security Program (NISP).

> For *Confidential and Secret information, the Defense Industrial Security Program requires that contractors be inspected every six months, that guards physically check safes that hold classified material, and that stringent document control audits and inventories be maintained. Director* of Central *Intelligence representatives normally inspect* facilities *housing Sensitive Compartmented Information once every two years, require*

alarms rather than expensive guards, and recently have dropped strict document handling requirements.

The Commission seeks to apply physical, technical, and procedural security consistent with the same basic risk management principles recommended throughout this report. Security standards should provide two uniform degrees of protection for classified information. Decisions to adopt special protection safeguards should be based upon risk management analysis of the value of the asset, the threats and vuinerabilities, and the costs of protection. The relationship between government and industry should be a problem solving partnership that maximizes reciprocity. New procedural mechanisms should be instituted to terminate unnecessary controls and facilitate ease of reassigning cleared personnel.

Physical Security Standards

Today's physical security policies evolved in the context of the Cold War when it was often assumed the enemy would attempt penetration and it was necessary to keep them out at almost any cost. Organizations began to individually adopt different rules governing the protection of classified information. As a result there is no single facility standard. Facilities cleared for DoD Special Access Programs have rules which may vary from facility to facility and from program to program. Facilities housing Sensitive Compartmented Information (SCI) are governed by the Director of Central Intelligence Directives. Facilities holding collateral information follow differing standards depending on which organization is the sponsor. Application of these differing standards by individual government agencies is also uneven, resulting frequently in one government agency being unwilling to share space with another agency even though they both ostensibly use the same standard.

A facility's security may include alarms, guards, security containers (safes), access control devices, closed-circuit television, locks, special construction requirements, and a host of other countermeasures. It also may include a requirement for two people to be in close proximity at all times so as to deter the unauthorized removal or copying of classified material. With total risk avoidance as the goal, the addition of each of these countermeasure is justified by assuming that the countermeasure will provide an additional measure of protection. Cost is not a factor.

The physical security countermeasures at one industrial facility include a fence, roving guards, and automated building access controls. Inside fhe facility, there is also a specially constructed room to which access is controlled by cipher and combination door lock. Moreover, the program manager of a special access program required that the five-drawer safe used to store program material have each drawer alarmed even though the safe was inside an area already alarmed.

Yet the great majority of past compromises have involved insiders, cleared persons with authorized access who could circumvent physical security barriers, not outsiders breaking into secure areas. We have had numerous incidents of classified information being removed by cleared personnel, but no documented evidence leading us to believe an agent of a foreign power has ever broken into a classified area inside the United States.

The great majority of past compromises have involved insiders, cleared persons with authorized access who could circumvent physical security barriers, not outsiders breaking in to secure areas.

In reviewing the existing standards for physical security and their implementation in practice, the Commission found that the amount of physical security provided to protect classified information in facilities within the United States is often excessive.

The Commission acknowledges the significant and ongoing policy changes affecting physical, technical, and procedural security requirements that are being developed, especially through the DCI Security Forum and the National Industrial Security Program task forces. Many improvements have already been introduced and some cost savings already realized. For example, the recent DCI policy decision to drop the two-person rule has permitted manpower savings in some contracts. Other elements, such as the military SAPs, continue to enforce this requirement. Not only do these inconsistencies produce confusion, they seriously erode the user's faith in legitimate security practices. Despite some positive efforts, the Commission concludes that many of the rules governing physical and technical protection of classified information stored within the United States have yet to realistically reflect the actual threat.

Multiple standards, variously interpreted have inhibited . . . the efficient sharing of facilities and services.

The Commission believes that an integrated systems approach based on valid risk management analysis must be implemented to replace the current fragmented process. Under risk management, each countermeasure can be viewed in the context of a fully integrated system. The introduction of two uniform degrees of physical security protection will remedy the current inconsistencies and permit the establishment of a more rational approach to the physical protection of information and material.

The Commission recommends that classified material or information stored within the United States be protected by one of two levels of a national physical security standard.

Facility Certification

Multiple standards, variously interpreted have inhibited, primarily in the DoD, the efficient sharing of facilities and services, resulting in increased cost to the US Government. Sharing is more prevalent in the Intelligence Community where areas used for storing and discussing Sensitive Compartmented Information (SCI) are built to standards contained in a DCI Directive. For years, these areas, called Sensitive Compartmented Information Facilities (SCIFs), have been certified by the first agency to use that particular space. Written agreements allow additional agencies to use the same facilities, accepting any waivers to the standards. Facility clearance reciprocity is less prevalent (but increasing) for Special Access Programs. All too often SAPs levy additional requirements by forcing contractors to add costly and excessive security upgrades or even build a new SCIF (or SARF-Special Access Required Facility).

One west coast contractor said that the Intelligence Community usually grants approval for co-utilizing SCIFs within 48 to 72 hours. Yet the same process usually takes 4 to 6 months *in* the SAP world. *Additionally,* SAP

program managers may levy further requirements, such as one manager who wanted $30,000 in upgrades made to an already accredited SCIF.

The Commission supports co-utilization of certified facilities and further believes a registration system would help enforce this process. Once certified, a facility should be registered in a central data base. All government organizations desiring to operate at the relevent security level should accept the registered area without changes, enhancements, or upgrades. The facility should also remain certified until it is modified or closed out. Co-utilization of facilities is endorsed by the NISP and this registration process would complement the NISP effort

The Commission recommends a data base registering certified facilities be established and **that co-utilization and reciprocity of accredited space be mandatory.**

Facilities, Containers, and Locks

While uniform standards are important, the standard itself must be sup ported by an analysis of actual threat and a reasonable risk management response. The importance of this is shown by the example of the national standard adopted for security containers and locks. Current national policy requires classified material be stored in GSA-approved safes or containers with approved locks. Exceptions to this policy were routinely made in domestic settings during the Cold War in acknowledgment that other layers of security were in place or because of site specific factors such as floor loading restrictions. Non-GSA-approved containers (bar lock cabinets equipped with changeable combination locks) and the open storage of classified information in specially constructed areas have been routinely allowed. There is no evidence that these waivers have compromised security. The risk management approach embodied in granting these waivers should become the basis for developing future policies. The Commission strongly opposes recent efforts that are calling for more stringent standards. An example is the current effort to replace existing container locks with the new GSA-approved electromechanical locks. This replacement effort is not based on current threat data and will significantly increase costs. For example, one west coast contractor estimates that replacing all the locks for its facility would cost more than $7.3 million. While new locks could be used in new containers, the Commission found no evidence that would warrant a large-scale replacement effort for locks already installed in approved facilities within the United States.

The Commission recommends that there be no replacement or retrofit of containers and locks currently approved for use in the United States.

Industrial Security Inspections

Companies with classified government contracts are periodically inspected to ensure they are protecting classified material in ways consistent with government security standards. These inspections take many forms to include an initial accreditation inspection, a change of status inspection when there is new ownership or new spaces, and special interest inspections based on a specific incident, investigative lead, or threat. In addition to these accreditation and incident-driven visits, there also are routine re-inspections required on a varying and arbitrary periodic basis depending on the contract and sponsor. These routine inspections are conducted by the DIS, the DoE, the CIA, the NSA, or any number of individual DoD SAPs, all using a variety of standards. The CIA and the DoE inspect every two years, allowing the contractor to self-inspect on the off years. Until recently, the NSA maintained a six month schedule. The DIS, responsible for the majority of the inspections, also reviews all aspects of a contractor's security program every six months. Less than one percent of these inspections result in unsatisfactory ratings. Both the frequency and **value** of these routine inspections were questioned by contractors interviewed by the Commission.

> ***One contractor stated that*** *in 2992, DIS spent 480 hours inspecting the* ***contractor's five facilities.*** *But in 1993, despite the contractor's* ***38-percent*** *reduction in personnel,* ***68-percent*** *drop in documents,* ***40-percent*** *less* ***controlled*** *area, and SO-percent* ***fewer classified*** *holdings, DIS needed* ***1413 hours*** *to* ***inspect the same five facilities.***

Contractors with Special Access Programs are inspected on a program-by-program basis with each individual project having its own requirements. For example, a contractor with six SAPs may undergo six separate inspections with each having differing requirements. Contractors state that routine re-inspections are time-consuming, onerous, costly, and confusing. They advise that the redundant inspections contribute little, if any, additional security.

Contractors state that routine re-inspections are time-consuming, onerous, costly, and confusing.

> ***One*** *contractor* ***had to*** *contend* ***with*** *26 inspections by DIS and SAPs over a IO-month period in 1993.* ***Inspectors*** *were* ***on-site for*** *99 out* ***of*** *210* ***work-days.*** *An* additional week *of planned inspection was canceled.*

Intelligence Community inspectors put less weight on fault finding and more emphasis on program review. For example, they may frequently visit a contractor to discuss programmatic or individual personnel security issues but rarely conduct formal top-to-bottom inspections. Some Intelligence Community components use award fee contracts with monetary awards as incentives for good security. The Commission endorses the partnership or service approach towards security, rather than an adversarial approach.

The Commission supports accreditation visits and special issue investigations, but sees no need for each organization to conduct routine inspections. These reinspections frequently involve a top-to-bottom review of construction, storage, and procedures complete with formal out-briefings to senior management. They also often require an official response ***from the*** senior management. Our vision of a government and contractor partnership rejects the concept of these punitive inspections. The Commission believes that multiple compliance inspections and re-inspections are costly, time consuming,

and of questionable value in providing better security. A partnership or service-based approach should be encouraged.

The Commission recommends that, after an initial accreditation inspection, reinspections be limited to aperiodic, random inspections or those in reaction to specific incidents or threats. Routine industrial security re-inspections should be eliminated.

TEMPEST

TEMPEST (an acronym for Transient Electromagnetic Pulse Emanation Standard) is both a specification for equipment and a term used to describe the process for preventing compromising emanations. The fact that electronic equipment such as computers, printers, and electronic typewriters give off electromagnetic emanations has long been a concern of the US Government. An attacker using off-the-shelf equipment can monitor and retrieve classified or sensitive information as it is being processed without the user being aware that a loss is occurring. To counter this vulnerability., the US Government has long required that electronic equipment used for classified processing be shielded or designed to reduce or eliminate transient emanations. An alternative is to shield the area in which the information is processed so as to contain electromagnetic emanations or to specify control of certain distances or zones beyond which the emanations cannot be detected. The first solution is extremely expensive, with TEMPEST computers normally costing double the usual price. Protecting and shielding the area can also be expensive. While some agencies have applied TEMPEST standards rigorously, others have sought waivers or have used various levels of interpretation in applying the standard. In some cases, a redundant combination of two or three types of multilayered protection was installed with no thought given either to cost or actual threat.

A general manager of a major aerospace company reports that, during building renovations, two SAPs required not only complete separation between their program areas but also TEMPEST protection. This pushed renovation costs from $1.5 million to $3 million just to ensure two US programs could not detect each other's TEMPEST emanations.

In 1991, a CIA Inspector General report called for an Intelligence Community review of domestic TEMPEST requirements based on threat. The outcome suggested that hundreds of millions of dollars have been spent on protecting a vulnerability that had a very low probability of exploitation. This report galvanized the Intelligence Community to review and reduce domestic TEMPEST requirements.

Currently, many agencies are waiving TEMPEST countermeasures within the United States. The rationale is that a foreign government would not be likely to risk a TEMPEST collection operation in an environment not under their control. Moreover, such attacks require a high level of expertise, proximity to the target, and considerable collection time. Some agencies are using alternative technical countermeasures that are considerably less costly. Others continue to use TEMPEST domestically, believing that TEMPEST procedures

Hundreds of millions of dollars have been spent on protecting a vulnerability that had a very low probability of exploitation.

discourage collection attempts. They also contend that technical advances will raise future vulnerabilities. The Commission recognizes the need for an active overseas TEMPEST program but believes the domestic threat is minimal.

Contractors and government security officials interviewed by the Commission commend the easing of TEMPEST standards within the last two years. However, even with the release of a new national TEMPEST policy, implementation procedures may continue to vary. The new policy requires each Certified TEMPEST Technical Authority (CTTA), keep a record of TEMPEST applications but sets no standard against which a facility can be measured. The Commission is concerned that this will lead to inconsistent applications and continued expense.

Given the absence of a domestic threat, any use of TEMPEST countermeasures within the US should require strong justification. Whenever TEMPEST is applied, it should be reported to the security executive committee who would be charged with producing an annual national report to highlight inconsistencies in implementation and identify actual TEMPEST costs.

Domestic implementation of strict TEMPEST countermeasures is a prime example of a security excess because costly countermeasures were implemented independent of documented threat or of a site's total security system. While it is prudent to continue spot checks and consider TEMPEST in the risk management review of any facility storing specially protected information, its implementation within the United States should not normally be required.

The Commission recommends that domestic TEMPEST countermeasures not be employed except in response to specific threat data and then only in cases authorized by the most senior department or agency head.

Few [bugs] are uncovered in areas where good physical security and access controls are in place and . . . the overwhelming number of technical attacks against US interests occur overseas.

Technical Surveillance Countermeasures (TSCM)

Technical Surveillance Countermeasures (TSCM) involves the search for technical surveillance devices or "bugs." The TSCM function is decentralized within the government and resources and requirements are determined at the department or agency level. Traditionally, TSCM teams conduct inspections of domestic facilities when they first open and on a routine basis thereafter. TSCM teams are also called upon when there is some indication of a threat. A recent classified study shows that over the last 40 years, initial and routine domestic inspections uncovered few bugs, with the exception of an occasional hazard such as an on-line telephone connection or a two-way intercom into a secure area. The study also notes that few finds are uncovered in areas where good physical security and access controls are in place and that the overwhelming number of technical attacks against US interests occur overseas.

The failure to discover any use of technical surveillance devices domestically, coupled with budgetary pressures, influenced the application of TSCM. Within the last two years, the interagency TSCM training academy and two technical security laboratories have had to curtail their operations because of lost funding.

Although there is little or no evidence of a domestic threat, the Commission believes that overseas locations can be very vulnerable to technical invasion. It is therefore very important to maintain an active, focused, interagency R&D program in support of TSCM. Scarce resources should be directed both to specific threat-driven inspections and to the maintenance of an R&D and training effort.

The Commission recommends:

a) The elimination of routine TSCM inspections within the United States in favor of increased emphasis on overseas inspections. Any domestic TSCM efforts should be specifically threat driven.

b) The government fund a coordinated TSCM R&D and training **program to support overseas inspections and as a defense against future technological advances in technical surveillance equipment.**

PROCEDURAL SECURITY

Central Clearance Verification

The verification of an individual's clearance and level of access is a **critical** component in the management of interagency and industry **visits** to classified areas. On any given day. **thousands** of clearance **access requests** are made. Hundreds of personnel are **officially** involved in clearance **verification.** Many more are involved peripherally, and failure of the process affects most cleared person2 at some point.

The typical visit request goes through at least six steps, involves **at least three** levels of **the bureaucracy at each agency,** and can take anywhere from one to three days. One security manager stated that she spends some **40** percent of her time handling visit requests, and, that she must rely on personal contacts and informal **channels** to get the job done. Considering the hundreds of visits conducted daily within the community, the productivity loss is enormous. All too often, individuals ask their security officer to pass **clearance information, and, when they arrive at a meeting location, they are told,** 'We **did** not receive your clearance, you cannot enter the building." A flurry of calls between the visitor and his security officer determines that the clearances were sent, despite the fact that the receiving office has no record of the incoming clearance. Time elapses, sometimes after heated exchanges, the clearance information is orally passed, and the meeting starts:

> *Despite having his clearance passed a week **before** a quarterly meeting at the CM, a senior military **officer** was delayed some 30 minutes while his **military** assistant, whose **certification was*** passed ***and*** received *at* the *same time, had no **difficulty** entering.*

The current clearance verification system draws upon clearance information contained in data bases maintained by the OPM, the **DoD,** and the CIA.

*The **typical** visif request goes through at least six **steps,** involves af least fhree levels of the bureaucracy af each agency, and can fake **anywhere from** one to fhree days.*

Some highly sensitive programs, for example, the DoD SAP community, also maintain clearance/access data bases that are withheld from the major data bases. The CIA community-wide data base for certifying access to Sensitive Compartmented Information (SCI) is obsolete and scheduled to be replaced within two years. The DoD's Defense Clearance Investigative Index (DCII) is being upgraded and will be interconnected with the Federal employment Suitability and Security Investigations Index (SSII) maintained by OPM. The DoD and the OPM data bases contain more than 95 percent of all collateral clearances. The proposed CIA system will include all of the SCI clearances. By combining these data bases and adding special programs, the user community would have a Central Clearance Verification System (CCVS). Such a system would reduce duplicative record systems, administrative processing, time delays, and personnel requirements. In addition, a central clearance data base would provide the information backbone for the application of "smart-card" technology for instant clearance verification (without human intervention) for access to networks, E-mail, and facilities.

The Commission recommends that a Central Clearance Verification data base be developed and made available to industry and government. The data base should contain all collateral and SCI clearances. Sensitive clearance information should be encrypted or otherwise protected within the data base.

Certification of Contractor Visits

The DoD industrial security rules require stringent control and prior approval of contractor visits, especially when classified information is to be discussed. Contractor visit requests must be provided, in writing, in advance of an **actual visit** However, under certain circumstances, contractor visit requests must also contain a signed certification from the cognizant government contracting officer or prime contractor that the visitor has a need-t* know under a particular contract for **access** to classified information. This policy does not apply to government employees.

Contractors question the need for the certification process in view of the heavy dependence of the process on paper.

The requirement to certify need-to-know for each individual visit request between contractors without a direct classified contractual relationship, has increasingly caused significant problems and needless delays. Contractors question the need for the certification process in view of the heavy dependence of the process on paper. They maintain that the advent of facsimile machines and data base management systems for transmitting visit requests renders the exercise of obtaining a contracting officer's signature on each paper visit request obsolete. Critics also cite the practical difficulty in locating a government authority to certify individual visits. In many cases, government certification of need-to-know is in fact a rubber stamp. In circumstances such as contractor attendance at classified symposia and conferences involving general technical areas or subjects unrelated to any particular classified contract, the certification rule becomes a real impediment to accomplishing normal, legitimate business.

The Commission believes that the requirement for need to know certifications for contractor visits involving generally protected projects is outdated, imposes a dual standard for government and industry security, and should be abolished. The process unnecessarily complicates and slows the accomplishment of necessary business and inhibits the exchange of information that should take place between properly cleared and accessed personnel. A requirement for government certification of a contractor's need to know should be restricted to those contractor visits or meetings involving specially protected projects, rather than a blanket requirement for all classified visits between contractors without a contractual relationship.

The Commission recommends that the requirement for government certification of need-to-know for contractor visits at the generally protected level be abolished.

Communitywide Badge Systems

Interagency access procedures established by various security organizations serve two basic functions: to verify a person's identity and to validate clearance level. Virtually all agencies controlling access to their facilities rely on badges (permanent staff and visitor), automated and /or guard access controls, and administrative procedures for certifying and transferring clearance information. Over the years, each agency has developed its own badging system, visitor control process, and escort requirement to restrict unauthorized access. When outsiders seek access on official business, however, the system frequently breaks down. Badges are unique to each agency and vary in sophistication, that is, from serving purely as visual recognition to offering considerable encoded information readable by automated equipment at the point of entry. Thus, the lack of standardization makes for cumbersome procedures and contributes to frequent visitor delay at entry points. In many instances, cleared personnel must complete the same forms, sign the same waivers, and adhere to the same escort requirements as uncleared visitors, despite having had their clearances passed. One security manager stated, "The visit processing procedure is a cottage industry in need of modernization."

The visit processing procedure is a cottage industry in need of modernization.

Several intelligence agencies (the CIA, the NSA, and the DIA) have recently adopted limited badge reciprocity in an effort to streamline interagency visit procedures. Critics of the reciprocity program contend that it is difficult to administer (too many badges for guards to remember, reader incompatibility, and so forth), and that variability in implementing reciprocity has exacerbated an already inefficient process. For example, a CL4 employee on an official visit to the NSA under the new badge reciprocity procedure must still visit the NSA central badge office, fill out and sign a form, get an NSA visitor badge, and wait to be announced to his or her host by the receptionist, exactly the same steps as would have to be performed if the visitor had no badge at all.

The Commission concludes that the current badge control procedures are costly and impede interagency business by authorized personnel. The Commission is aware that the DCI Security Forum has tasked the NSA with devel-

opment of a community badge and that similar efforts are under way within the DoD and the DoE. These efforts should be coordinated and combined to provide a single-badge standard throughout the security community.

> The Commission recommends the development of a uniform badge system for the government's cleared community. The **badge system should provide for visual and electronic recognition, automated access control, and** encoded level of access.

The elimination of document tracking would not degrade security but could result in substantial savings.

Document Tracking and Control

The DoD Industrial Security Manual (EM) requires itemized **accounting** and verification of Secret documents held by industry in support of classified contracts. The DoD does not apply this standard internally. Neither the DoE nor the CIA have this requirement for their contractors, and the Director of Central Intelligence just approved the NRO's request for elimination of this requirement for certain Secret SCI documents. Moreover, the Task Force on **Classification** Standards recommended that accounting or strict tracking requirements for Top Secret material in SCI facilities be eliminated.

Contractors contend that document tracking and inventory requirements do not enhance security and are very costly One major contractor estimates a single classified document requires 98 minutes handling time annually. Results from an informal survey conducted by the Commission suggest that eliminating the requirement to precisely track every Secret document could reduce document control personnel staffs by some 40 percent. Most contractors would continue to maintain a basic data library function, but security requirements for extensive inventories and recording of internal transfers would be eliminated.

A number of senior government officials similarly have questioned the cost effectiveness of this type of document accountability. Some have opined that it is an expensive control system but that they know of no case in which document accountability has led to the identification of a spy. We have heard that when accountable documents are missing, time-consuming inquiries inevitably led to the conclusion that the material was "inadvertently destroyed." One senior official has stated that the elimination of document tracking would not degrade security but could result in substantial savings if manpower associated with the current process is eliminated.

Contractors **also** object **to the** need for extensive **justification** and protracted negotiations currently required for retention of classified documents when a contract is completed. They must frequently "reinvent the wheel" because information generated for one contract cannot be used in performance of another. Required to turn information in at the completion of a contract, a contractor must then approach the government and ask for the product that was originally generated by the contractor. Contractors also note **that the** regulations are inconsistent, providing for retention of R&D classified information but not routine contract materials.

The Commission believes that the integrity and trustworthiness of personnel is the key to the proper protection of documents. Strict document

accounting and retention practices are costly and do not deter compromise of information. To those who would cause damage, personal computers, facsimile machines, copier equipment, and modems and networks, available in the normal office environment, offer opportunities to compromise documents without detection despite elaborate and costly physical document accountability and control procedures.

The procedures mandated by the DoD Industrial Security Manual to account and track documents do not provide real protection. There is no value in accounting for the physical possession of 100 documents in the morning and 100 at the end of the day if at midday they can be copied electronically without detection and transmitted to an unauthorized party. There is no evidence that the lack of tracking of Secret documents in government offices has led to an increase in compromises. The industrial standard should be no different.

The Commission recommends that:
a) The requirement for internal tracking and inventory and periodic inspections of classified documents be eliminated.
b) Contracts be amended to allow routine retention of classified documents provided that they are properly safeguarded.

Document Destruction

There are also similar accounting and verification requirements for the destruction of classified documents. DoD internal regulations generally require records of destruction and the imposition of the two-person rule for Top Secret documenk destroyed by government employees. There is a two-person rule but no destruction record required for Secret documenk, and only one cleared person is required to destroy Confidential documenk.

The DoD Industrial Security Manual requires destruction records and the two-person rule for destruction of both Top Secret and Secret documents; only one person is required to destroy Confidential documents. The DoE does not require records of destruction for either Secret or Confidential.

For SCI documenk there generally is no requirement for destruction certification, but there is a two-person rule.

The same logic that compels us to recommend the elimination of document accountability drives the conclusion that document destruction accountability requirements are a cost without a significant benefit, and the requirement should be eliminated. Anyone who wants to remove classified information can do so while leaving the accountable record copy untouched and then properly accounting for its destruction. Destruction records, which must be duly dated, signed, and retained, and the two-person rule represent avoidable costs that give no more than an illusion of security.

Destruction records, which must be duly dated, signed, and retained, and the two-person rule represent avoidable costs that give no more than an illusion of security.

The Commission recommends that item-by-item document destruction accountability be eliminated.

Document Transmittal

The expense of using couriers or hand carrying all specially profecfed informa fion is unwarranted in mosf cases.

In the current environment, encrypted data transmission should be the rule. Expensive, labor and time intensive document transmittal by mail service or courier should be the exception.

To the extent that it is necessary to utilize older methods of document transmittal, we recommend a standard be adopted for generally protected information and one for specially protected information.

Currently DoD internal regulations allow Confidential documents to be transmitted in US postal channels either by first class mail or by certified mail; Secret documents must be sent by registered mail; Top Secret, SCI and SAP documents must either be sent by courier or hand-carried by appropriately cleared and authorized **persons. The Industrial Security Manual requires use** of US postal service express or registered mail for Secret and certified mail for Confidential documents.

The Commission believes there are no significant risks in routinely using registered or certified mail for transmitting generally protected information. **In some cases, first class mail** or **commercial services are adequate.**

The Commission also believes that the expense of using couriers or hand carrying all specially protected information is **unwarranted in** most cases. Registered mail is used to safely transport expensive jewels and high-value negotiable instruments. At the specially protected level, managers should also have the option of using certified or registered mail instead of being forced to use expensive couriers. While the Commission believes transmission options should be expanded, the decision on which mode is best suited for individual programs should be made at the local level.

The Commission recommends that the document transmittal rules be revised for both generally protected and specially protected information. Generally protected documents should be sent by US first class, certified, or registered mail, or by a commercial delivery service. Specially protected documents should be sent by either US registered mail or by courier.

Operations Security

Some elements of the intelligence and defense community have been using the risk management process for many years under the rubric of Opera-

tions Security (OPSEC). Growing out of lessons learned in the Vietnam war, OPSEC seeks to "control information and observable actions about one's capabilities, limitations, and intentions so as to prevent or control their exploitation by an adversary."[14] Emphasis is placed on the analysis of unclassified information and public sources.

Seeking to institutionalize this process, in 1988 National Security Decision Directive (NSDD) 298 mandated the implementation of a formal OPSEC program by each executive department and agency with national security responsibilities. It designated the Director of NSA as executive agent for OPSEC programs and tasked him to establish and maintain an Interagency OPSEC Support Staff (IOSS)[15] to provide consultancy and training for executive departments and agencies required to have formal OPSEC programs.

The Commission believes that there is a clear and compelling need for operational security in a military environment and in the conduct of sensitive operations. However, in the years since the establishment of the National Operations Security Program, a formal OPSEC structure has developed apace, with OPSEC responsibilities being assigned at each organizational level of DoD service departments and agencies, at the DoE, and at other government departments and agencies. There is now a robust OPSEC community coexisting with, but for the most part, separate from the standard security structure. The OPSEC Professionals Society boasts of a membership of some 475 professionals, with membership being equally divided between government and the private sector.

OPSEC.. . is seen as a separate discipline not integrated with other security disciplines and competing with them for scarce resources.

OPSEC is perceived by many, particularly in industry, as just a new way to repackage security requirements using elaborate procedures. It is seen as a separate discipline not integrated with other security disciplines and competing with them for scarce resources. National OPSEC requirements are framed in such general terms as to provide insufficient guidance for program managers and resource allocation. Moreover, despite the NSA's training of over 2,200 individuals in the OPSEC process over the past 3 years, industry sources advise that government security managers, contracting officers, and program managers are not trained in and do not understand OPSEC methodology, rarely request OPSEC surveys, do not provide specific threat data, or inspect for OPSEC compliance.[16] To meet the demands of government contracts, industry, which also has a shortage of experienced OPSEC people, must recruit and train people to provide consultant support to ongoing classified industrial programs at unwarranted expense.

No one interviewed by the Commission questioned the appropriateness of selecting cost effective security countermeasures based on the assessment of risk. What is questioned is the wholesale imposition of the separate OPSEC structure to all sensitive governmental activities, including classified contracts with industry. OPSEC should not be a separate program, but part of the risk management philosophy that is integrated throughout the existing security structure.

The Commission recommends that:

a) The norm4 security staff structure and risk management processes be incorporated into security and security awareness training programs at all levels.

b) Mandatory requirements for formal OPSEC programs be deleted from all contracts except those in response to specific threats and then only when specifically authorized by the most senior department or **agency head.**

c) NSDD 298 be reviewed, revised, or rescinded in accordance with these new requirements for OPSEC.

Chapter 6.

Protecting Advanced Technology

With the end of the Cold War and facing new challenges to US economic competitiveness, policymakers are focusing on the threat from foreign government and nongovernment entities to US advanced technologies, defense-related industries, proprietary data, intellectual property rights, and trade secrets. The increased value of US technical information necessitates balancing national policy objectives and the importance of sharing information with the need to protect our leading edge technologies.

Highest priority is given to limiting the proliferation of weapons of mass destruction and advanced conventional weapons. Counterproliferation and nonproliferation policies range from diplomacy and export control regimes to the development of new weapon systems and tactics to counter advanced foreign systems on the battlefield. Negotiating and implementing a new international export-control framework is a complex task, and bringing consistency and coherence to US export-control policy requires the resolution of sharply conflicting interests. Both require an overall strategic direction that is beyond the Commission's mandate. The Commission has focused on a smaller segment of the counterproliferation policy spectrum, specifically the policies and procedures regarding foreign ownership or control of industrial firms performing classified contracts, military exchanges with foreign governments, and national disclosure of classified information to permit export and coproduction of classified weapon systems.

The risk in each of these situations is that foreign entities will exploit the relationship in ways that do not serve our overall national goals of preserving our technological advantages and curtailing proliferation. These goals generally include keeping certain nations from obtaining the technical capabilities to develop and produce advanced weapon systems and from acquiring the ability to counter advanced US weapon systems. In cases where US national interests require the sharing of some of our capabilities with foreign governments, security safeguards must ensure that foreign disclosures do not go beyond their authorized scope. Safeguards must also be tailored to new proliferation threats and applied effectively to the authorization of foreign investment in classified defense industry and the granting of access by foreign representatives to our classified facilities and information.

Security safeguards must ensure that disclosures do not go beyond their authorized scope.

The Commission notes an additional area that is beyond the scope of this report but merits further attention. This issue is the need to update counterproliferation guidelines for prepublication review of reports of scientific and technical research funded by the government. Such matters involve the delicate balance between our paramount national commitment to an open scientific community and the imperative to control the spread of weapons of mass destruction by limiting access to unclassified but high-risk data. Improved

protection of classified technology, as proposed by the Commission, is only one part of the comprehensive counterproliferation program that our nation requires.

Foreign Ownership, Control, and Influence

A basic tenet of our industrial security policy is that business firms engaged in classified government work should be controlled by persons who can be trusted to safeguard classified information. DoD policy, for example, requires that any company bidding on classified contracts must hold a facility security clearance issued by the government. The DoD also requires that the firm should not be subject to undue control or influence by foreign investors. When a foreign investor buys or otherwise acquires influence over a US company, the retention or initial issuance of a facility clearance is dependent upon a favorable Foreign Ownership, Control, and Influence (FOCI) determination. During the Cold War, regulatory policies governing FOCI determinations ranged from total risk avoidance to risk acceptance. For example, FOCI policy prohibited Soviet and other Communist countries from having a financial interest in, or otherwise influencing, US companies. However, with respect to non-Communist countries, especially our allies, special procedures were developed to mitigate FOCI in order to permit foreign investment without compromising classified information

Until 1992, there was a growing effort to accommodate the desires of foreign investors so as to encourage the infusion of capital and the development of joint projects to exploit technologies and markets to the benefit of both US companies and their foreign investors. A controversy arose in 1992 when a foreign firm that was majority owned and controlled by a foreign government sought to acquire a leading US defense company performing work in support of highly classified programs. Questions were raised about the sufficiency of traditional FOCI security arrangements (generally legal instruments to insulate US managers and workers from foreign owners or limit the scope of classified contracting)[21] to protect classified leading edge technology from foreign exploitation.

The case triggered a DoD and Congressional review of FOCI policy and reflected a growing concern over foreign economic espionage aimed at advanced US technology. As a result, the DoD drafted a proposed new FOCI policy, but the proposal proved controversial and was shelved, waiting in part for the recommendations of this Commission. Congress also enacted legislation in 1992 barring foreign government-controlled companies from acquiring US companies engaged in classified contracts unless the transaction is approved in accordance with the Exxon-Florio Amendment[22].

The Commission supports foreign investment in the US defense industry base but believes that FOCI policy should ensure that foreign firms cannot undermine US security and export controls to gain unauthorized access to critical technology. Essential to a sound policy is current intelligence, counterintelligence, and law enforcement information on attempts by foreign governments and commercial interests to obtain such access. This requires a closer relationship between the industrial security programs and the Intelligence community.

FOCI policy should ensure that foreign firms are denied the opportunity to undermine US security and export controls to gain unauthorized access to critical technology.

The Commission found that policymakers do not always have the information necessary to make sound and timely FOCI decisions. Comprehensive counterintelligence or intelligence information as to ultimate ownership, much less control or influence, is not centrally collected, analyzed, and made available to FOCI decision makers. The absence of a centralized FOCI decision data base also limits the flow of information and slows FOCI determinations. Legal review of contract documents enunciating security provisions to isolate FOCI is performed by the CIA, the DoE, and the DoD. However, within the DoD, FOCI contract documents are not consistently submitted for review by experts in the DoD's Office of General Counsel.

The Commission also found that there is no coherent national policy on FOCI. When foreign investment is sought in US industries that work with the Defense and Intelligence Communities, FOCI decisions are independently made by the DoD, the DoE, and the CIA. Each has its own procedures for developing and evaluating available threat information, devising an acceptable security arrangement, and monitoring compliance. For example, DoD FOCI determinations are made on a company by company basis whereas the CIA's determination is on a procurement by procurement basis. Moreover, an agreement such as the DoD's Special Security Agreement (SSA), is not acceptable to the CIA and the DoE because the SSA allows the foreign investor to exercise considerable management control over the US company. The CIA believes this approach does not totally negate FOCI-related security problems. Thus, a major US firm with multiple contracts sponsored by the DoD, the DoE, and the CIA may be subject to more than one FOCI arrangement.

The lack of a common FOCI policy contributes to a lack of reciprocity among government agencies and may also place certain companies at a competitive disadvantage.

The lack of a common FOCI policy contributes to a lack of reciprocity among government agencies and may also place certain companies at a competitive disadvantage. For example, the CIA judged one company a significant FOCI risk, but this did not stop the NSA from letting an unclassified but sensitive contract with that same firm. Although a common FOCI policy is being considered by the DoD, the DoE, the CIA and industry, there is no coordinating mechanism to ensure that the policy will be implemented, uniformly applied, and enforced.

The Commission recognizes that foreign investment can play an important role in maintaining the vitality of the defense industrial base. The existing FOCI policies and the political climate since the 1992 controversy have discouraged foreign investment. However, as a matter of policy, DoD has a number of programs to encourage cooperative international R&D and procurement with our allies to spread the burden of increasing costs and decreasing defense budgets. The Commission encourages these efforts and believes that FOCI policy should not undermine them.

The Commission also believes that "buy American" provisions, which preclude foreign firms from competing for US government contracts, must be used only when US national security interests would truly be threatened by foreign participation. "Buy American" restrictions should never be used for protectionist purposes. Finally, the Commission notes that international defense trade is increasing and that measures taken by the United States can invite retaliatory action by other nations that would harm US economic and security interests.

The Commission believes that the security executive committee should, as a key priority, develop a policy and a mechanism to balance these compet-

ing interests. The policy should be based on a risk management approach that permits departments and agencies to tailor the measures that are needed in an individual transaction. Rigid structures that inhibit foreign investment should be avoided.

The Commission **recommends that a coordinated FOCI policy be developed by** the security executive committee.

Foreign Exchange Agreements-The Status Quo

The United States is losing more than it is gaining through participation in many foreign exchange agreements.

Our foreign economic competitors focus a considerable amount of their collection efforts on United States leading edge technology and defense-related **industry Information** is obtained both overtly and covertly. Foreign liaison and cooperative exchange programs, such as the Defense Development Exchange Program (DDEP) and the Personnel Exchange Program (PEP),[23] allow the United States to exchange information concerning military, technical, or scientific data; weapons; weapon systems; or operational concepts with its allies. However, the Commission has come to believe that the United States is losing more than it is gaining through participation in many foreign exchange agreements. These programs, designed to better marshal the technological capabilities of the United States and **its allies, as well as to** reduce costs, have also served as vehicles for covert exploitation of our most sensitive technologies.

Foreign governments frequently stretch the boundaries of intergovernmental program relationships with aggressive, persistent, and coordinated efforts to gain **access** to nonreleasable technological data that they can use to further economic competition with the United States. This can be accomplished through international data exchange programs, which have grown tremendously over the past 30 years as more and more industrial countries seek advanced US technologies. There are approximately 750 DoD-wide agreements, with over 310 data exchange agreements in one military service alone.

Foreign liaison officers working within key DoD organizations can gain knowledge and invaluable insight into US leading-edge technology programs under development. Within one military service, approximately 118 foreign military personnel from 19 countries work under the Personnel Exchange Program; 43 foreign scientists or engineers from 6 countries work within its research and development facilities; and 172 foreign liaison officers officially representing 22 countries are integrated within various other service elements. Often, foreign governments use this insider knowledge to target and pursue technical information early in a major acquisition systems life cycle and then work against civilian targets, such as DoD contractors and university scientists engaged in defense work. Foreign liaison officers can also exploit their official status to gain 'back door" access to special access program technologies:

> *On several occasions, when a foreign liaison officer's request for sensitive technical infonnation was* denied *by one military command,* the *same request would surface through another foreign liaison officer at another*

command. In one instance, the second request occurred within one day of the first denial.

Critics of the Defense Development Exchange Program maintain that the program has become a one-way street for foreign governments to funnel United States advanced technology overseas, while providing comparatively little of value to the United States in return. A US Army Intelligence study[24] found that valuable classified and unclassified underlying technologies in many advanced weapon systems not authorized for release are being lost to foreign governments through the Defense Development Exchange Program These losses may eventually compromise our weapon systems and erode our technological superiority on the battlefield, or at the very least, provide advanced technology to US economic competitors.

The Commission recommends that the Secretary of Defense review existing data exchange programs, using updated threat information, to determine whether the programs should be continued, canceled, or renegotiated to ensure they are in concert with current US national security and economic goals.

Threat Analysis-Vital to Protecting Advanced Technology

The Commission recognizes the gravity of having leading-edge technology and weapons in the hands of foreign adversaries. However, the foreign exchange approval authorities of the military services generally make their determinations within the acquisition or international programs community and without participation by security, intelligence and counterintelligence elements. Moreover, these authorities often do not ascertain the impact of proposed technology releases on the security of related future weapons or weapon support systems. Intelligence and counterintelligence support elements can assist in devising the most effective course of action to deny foreign collection efforts. Threat information is available through the DCI's Nonproliferation Center, the DIA's National Military Intelligence Production Center, and the CIA's Directorate of Intelligence. The Commission's proposed interagency counterintelligence "one-stop shopping" effort will also provide a focal point for obtaining threat information needed for national level security policies.

For most organizations below headquarters level, however, the need is for information on the local threat to technologies under development or to critical facilities, rather than information pertaining to the broad national threat. Field organizations maintain that, to be of value, threat assessments must specify the foreign entity involved, identify what programs or systems it is targeting, and identify the specific areas of the country in which adversaries are operating. As a first step in meeting the local need, the DoD should modernize its counterintelligence collection and reporting system to speed the flow and improve the quality of both raw and finished counterintelligence products into a pull-down data base network. Counterintelligence elements should then work in daily partnership with field elements to explain the issues associated with protecting particular systems, provide practical local

soiutions, and serve as a valuable feedback mechanism in the total security process.

The Commission believes the military services' counterintelligence elements must work closely with the FBI with these concerns in mind, so as to ensure a seamless, integrated capability and a consolidated FBI, DoD, and defense industry network against economic espionage.

The Commission recommends that the Secretary of Defense direct that comprehensive, coordinated threat analysis, intelligence, and counterintelligence support be provided to facilitate risk management for DoD critical technologies, systems, information, and facilities.

The National Disclosure Policy

The National Disclosure Policy (NDP),[25] established under a Presidential dive, provides the framework for approval or denial of disclosure of classified military information to foreign governments and international organizations. It also governs the export of classified military articles and unclassified military articles with embedded classified components. The Secretaries of the military departments have been delegated authority to render decisions with respect to disclosure of their information to the governments of most countries with which the United States has mutual defense arrangements. In the case of other countries an exception to policy is usually required. Exceptions to policy may be approved when it is determined that the proposed export or disclosure will result in benefits to the US Government that outweigh the damage that might accrue to US foreign policy, national defense, or military operational interests if the system or its underlying technology should be compromised.

The Commission notes that the National Disclosure Policy Committee (NDPC), chaired by the DoD, coordinates foreign release policy and government-to-government agreements. Exceptions to the National Disclosure Policy receive senior-level review within the DoD as coordinated by the NDPC. However, most routine release decisions are made by field elements under authority delegated by the Secretaries of the military departments. This decentralized execution leads to different interpretations as to what is releasable within the broad outlines of the NDP and consequently, different actual release decisions. Moreover, the Commission found that specific senior-level review decisions have not always been communicated to the midlevel acquisition or international program officials within the military services, who over the years have made the day-to-day disclosure decisions under specific data exchange agreements. A lack of understanding of the foreign disclosure process by less-senior individuals, combined with the absence of current threat assessments and an automated DoD data exchange process, prevents effective and consistent execution by elements involved throughout the DoD and the military services.

Specific senior-level review decisions have not always been communicated to the mid-level acquisition or international program officials.

The Commission recommends that the Secretary of **Defense:**

a) Centralize' responsibility for coordinating and overseeing all foreign exchange programs and issues at a senior level.

b) Improve and modernize the National Disclosure Policy process to ensure that senior-level disclosure decisions are readily available through a centralized, dynamic, interactive computer-driven mechanism.

The critical foreign exchange information contained in the FORDTIS data base should be made available to more DoD consumers.

Recording Foreign Disclosure Decisions

The Commission commends the DoD for **creating the** Foreign Disclosure and **Technical Information** System (FORDTIS) data base to house decisions of foreign release determinations and exceptions to foreign disclosure policy, technology transfers, and official foreign visits. The Commission supports the DoD's ongoing expansion of FORDTIS to military warfighting elements, such as US combatant commanders, to aid in determining specific classified and unclassified technologies or **weapon systems that are** releasable to foreign coalition partners. However, the Commission believes that the **critical foreign** exchange information contained in the FORDTIS data base should be updated and made available to more DoD consumers to aid them in analyzing, programming, and planning activities. Counterintelligence elements, in particular, should use the FORDTIS data base in determining the current status of releases of US technologies and systems.

The Commission recommends that the Secretary of Defense:

a) Expand access to the Foreign Disclosure and Technical Information System (FORDTIS) data base to command and other DoD consumers to support defense planning, programming, resourcing, analysis, and information-sharing activities.

b) Ensure counterintelligence elements cross-check critical systems or technologies against the Foreign Disclosure and Technical Information System (FORDTIS) data base to determine:

1) the extent to which baseline technologies on each system have been released to foreign nations, and;

2) the vulnerabilities posed to current or future weapons or weapons support systems if exchanges continue under the applicable Defense Development Exchange Program agreements.

Chapter 7.

A Joint Investigative Service

One of the more effective means of reducing overall personnel security costs, while enhancing the security posture of our nation, would be to reorganize current investigative resources and thoroughly modernize the process of gathering, investigating, reporting, and storing background investigative information.

The Commission has examined the organizational arrangements in the Department of Defense and the Intelligence Community for the performance of personnel security background investigations and industrial security functions. The Commission believes that the effectiveness of these activities can be substantially improved by the establishment of a new joint investigative service.

For the DoD, virtually all personnel security background investigations for civilian, military and contractor personnel are conducted by the Defense Investigative Service (DIS). In the Intelligence Community, personnel security background investigations are conducted by the DIS for the DoD component, including the NSA and the DIA. The CIA and the NRO have their own internal organizations that conduct or contract out background investigations for their employees and contractor personnel. The NSA also has an internal investigative organization that performs a limited number of background investigations.

The DIS also performs, for the DoD, all initial industrial facility certifications which establish that a contractor facility is eligible to receive classified information. The DIS then performs a full range of industrial security functions, such as periodic inspections and assistance visits, for all cleared facilities except for all Navy special access programs and for certain Air Force special access programs. This contrasts with the Intelligence Community's decentralized approach that emphasizes integration of security with program management teams.

Personnel Security Investigations

The Commission believes that one of the more effective means of reducing overall personnel security costs, while enhancing the security posture of our nation, would be to reorganize current investigative resources and thoroughly modernize the process of gathering, investigating reporting, and storing background investigative information. A previous section of this report outlined the substantial savings to be realized through improving the timeliness of the investigative product. However, we also heard from the end users that the investigative products they receive are uneven in quality and completeness. because of this, organizations often upscope investigations completed by other investigative organizations, or otherwise invest in additional types of vetting mediums, to establish greater confidence in their personnel. For example, a major SAP contracts out investigations rather than take advantage of "free" investigations provided by the DIS because of concerns about quality and timeliness.

The Commission believes that establishing measurable objectives to improve the timeliness and quality of investigations offers a solution to at least part of the problem. However, the current deficiencies and impending budget reductions casts doubt on improving the situation under the present organizational structure. For example, the DIS faces a 25 percent budget reduction over the next 4 years. Therefore, the Commission believes decisive and innovative action must be taken to resolve these problems.

The Commission proposes forming a new joint personnel security investigative organization for the DoD and the Intelligence Community. A new organization is needed to: establish progressive leadership; realize savings in manpower and personnel; maximize economies of scale; achieve commonalty of product; provide a single focus for implementing technological improvements and efficiencies; and enhance professionalism and career opportunities.

The new joint investigative service would be charged with conducting all personnel security background investigations for military members, civilian employees and contractors of the DoD, the CIA, the NRO, the NSA and all other entities reporting to the Secretary of Defense and the Director of Central Intelligence. The only exceptions to the investigative jurisdiction of the joint investigative service should be: 1) investigations of cabinet officials and political appointees currently performed by the FBI; 2) investigations of new civilian employees hired into the DoD and the Intelligence Community who occupy nonsensitive positions and, therefore, fall under the jurisdiction of the OPM, and; 3) personnel specifically exempted by the Director of Central Intelligence.

The Commission proposes that the joint investigative service be established by incorporating the personnel security investigative elements and resources of the DIS, the NSA, the NRO and the CIA. The Commission further recommends that the joint investigative service be staffed with both full-time investigators and rotational personnel from the security offices of the various agencies that it serves. This would facilitate communication between the investigative agency and its customers, and would provide government security officers with an opportunity to gain valuable investigative experience. The joint investigative service should also establish specific units to handle individuals with cover considerations, reporting these investigations through secure channels. Moreover, the joint investigative service would contract out domestic investigations when appropriate, such as priority investigations, and pursue overseas leads using m-place military and government resources on a reimbursable basis. However, individual agencies would continue to conduct their own special investigations, such as counterintelligence and criminal investigations, and perform their own adjudications.

The Commission believes that the joint investigative service should be industrially funded. The most efficient and customer responsive agencies are those that operate on a fee-for-service basis. For example, the Commission learned that until the OPM became industrially funded, it had a relatively poor reputation for delivering a timely, quality investigative product. Since instituting a revolving fund mechanism, the OPM has cut investigation times dramatically, initiated many innovative automation linkages with customer agencies, and, according to customers, improved the quality of its investigations.

The new joint investigative service would be charged with conducting all personnel security background investigations for milita y members, civilian employees and contractors of the DoD, the CIA, the NRO, the NSA and all other entities reporting to the Secretary of Defense and the Director of Central Intelligence.

The Commission recommends that a joint investigative service be established that performs all personnel security background investigations on a fee-for-service basis for the DoD, the NSA, the NRO, the CIA and other organizations that report to the Secretary of Defense or the Director of Central Intelligence.

The program-oriented approach ... makes security directly accountable for the quality and timeliness of its service.

Industrial Security

With respect to industrial security, the Commission found two distinct approaches to the protection of classified information by contractors: centralized and decentralized. The CIA, the NRO, the NSA and some of the DoD special access programs integrate security into program management. This decentralized approach integrates small security elements into program management teams with core security functions provided by a centralized service. Security is part of the program management team and provides direct support to organizational goals. The disadvantage of this approach is that it has, in some cases, worked against standardization and reciprocity. Particular SAP program offices have adopted their own security procedures. The centralized approach embodied in the DIS seeks to leverage limited resources through standardized practices and procedures, generally independent of specific contracts or programs. Disadvantages of a centralized approach include inflexibility, distance from the customer, lack of direct accountability, and a system based on achieving security goals independent of organizational goals.

On balance, the Commission has found the programmatic approach to industrial security to be superior to the traditional centralized approach of frequent inspections to measure compliance with a detailed manual of security rules. The program-oriented approach brings security closer to the customer and provides greater flexibility to handle program issues. This structure also makes security directly accountable for the quality and timeliness of its service. Contractors appear to prefer the flexibility of a programmatic approach, but insist that common standards are needed for reciprocity.

The Commission believes that a core industrial security function located within the joint investigative service would benefit the Defense and Intelligence Communities. The new organization should be responsible for initial facility clearances, for the previously recommended facility registration data base, and for all determinations concerning foreign ownership, control and influence (FOCI), as discussed earlier in chapter 6. The new organization should provide an industrial security service to those Defense and Intelligence Community program offices for which a joint industrial security program is most effective. It would also provide this service to non-Defense and Intelligence Community agencies, as the DIS has done in the past. It will centralize, as a core service, the staff to provide accreditation of facilities, technical and computer security expertise, guidance to handle treaty inspections, central records, and representation to industry and government forums. The new organization should promote standardization and responsiveness to customers and coordinate the industrial security inspections previously discussed in chapter 5. It should draw upon the experience of the industrial

security program of the NRO, which has made great progress in recent years in combining a programmatic orientation with greater standardization.

The Commission emphasizes that the new organization must break with the past practices which have tended to focus on frequent inspections for compliance with a detailed regulatory manual. Industrial security should be a service to the contract program office, with security performance measured in terms of mission accomplishment rather than adherence to detailed security rules. The joint investigative service should view its industrial security functions as a service to be used where a joint organization is more efficient and economical. The Commission does not intend to force into joint organizations those program offices in the CIA, the NRO, the NSA and certain SAPs that function better by maintaining their own industrial security capabilities. The Secretary of Defense and the Director of Central Intelligence will retain the discretion to authorize separate industrial security offices for specific programs.

The Commission recognizes that this decentralization of execution of industrial security runs a risk that general standards will not be applied uniformly. Indeed, a major disadvantage of the separate SAP industrial security programs in the past has been their adoption of unique security procedures that added multiple burdens to industry which translated into increased, unjustifiable costs to the government. One purpose of establishing a single classification level with two degrees of protection is to standardize the security requirements for the controlled access programs. The security executive committee should ensure that the standards are applied properly, and the joint investigative service should provide a channel through which industry may bring concerns to the attention of the security executive committee.

The **Commission recommends that a joint investigative service perform** industrial security services of **common concern for the Defense and Intelligence Communities, as determined by the security executive committee and in accordance with a programmatic, customer-service approach.**

Establishment of a Joint Investigative Service

For the reasons set forth above, the Commission has concluded that the Secretary of Defense and the Director of Central Intelligence should establish a joint investigative service to conduct all personnel security background investigations and updates for components of the Department of Defense and Intelligence Community, as well as their contractors, and to perform those industrial security functions that can better be done jointly. The advantages include economies of scale, greater commonality, more uniform implementation of standards, and increased professionalism and career opportunities.

The new organization should draw its personnel and resources from existing security organizations in the Defense Department and Intelligence Community. It should take its policy guidance from the security executive committee. While the Commission does not wish to prescribe the organizational details for a joint investigative service, one model is the Central Imag-

The advantages [of a joint investigation service] include economies of scale, greater commonality, more uniform implementation of standards, and increased professionalism and career opportunities.

ery Office (CIO). The Director of the CIO is appointed by the Secretary of Defense on the recommendation of the Director of Central Intelligence. Consideration should also be given to other joint DoD-DCI models that have been adopted for different functions. The joint investigative service could report to the Secretary of Defense and the Director of Central Intelligence directly or through a senior official designated by them. Above all, the Commission urges that the establishment and direction of the joint investigative service receive sustained, high-level attention, which has not been the case with the Defense Investigative Service over the years.

The Commission recommends that the joint investigative service be established by the Secretary of Defense and the Director of Central Intelligence, that its resources be drawn from existing security organizations, and that it report jointly to the Secretary of Defense and the Director of Central Intelligence.

Chapter 8.

Information Systems Security

Those who s feadfasfly resist connectivity will be perceived as unresponsive and will ultimately be considered as offering little value to their customers.

Information systems security is the discipline that protects the confidentiality integrity and availability of classified and unclassified information created, processed, stored and communicated on computers and networks. The Commission believes it is imperative that the Defense and Intelligence Communities focus more attention on information systems security It, together with personnel security, is one of two security disciplines that the Commission believes needs more attention and recommends additional requirements that will increase costs.

The United States is increasingly dependent on information systems and networks. Information systems control the basic functions of the nation's infrastructure, including the air traffic control system, power distribution and utilities, phone system, stock exchanges, the Federal Reserve monetary transfer system, credit and medical records, and a host of other services and activities. The world of the future, within which our security policies and procedures must succeed, will undoubtedly be characterized by even more widespread use of computers, systems, and networks. It is already apparent that increased connectivity leads to significant improvements in productivity, improvements that are necessary if our society is to prosper and we are to continue to lead the world's family of nations in economic, political, and military strength. Initiatives like the National Information Infrastructure (NII) intended to be an "information superhighway" for our nation's commerce and government are based on this emerging reality,

The Defense and Intelligence Communities share this imperative to connect, both within and between the communities and to the NII. The Department of Defense already depends upon computers and communications networks in performing every aspect of its complex missions from command and control, to acquisition of weapons systems, to managing and paying for the worldwide activities of the department. This dependence will certainly increase. The DoD envisions a worldwide, seamless web of computers and networks the Defense Information Infrastructure (DII) operating as a utility in support of the Department's warfighting, intelligence, and business functions.

The CIA and other intelligence agencies are increasingly tying together internal systems and are beginning to reach for connections beyond their walls. The increased productivity that flows from such connectivity is essential to success in this era of declining resources. Intelligence is, after all, information and must flow in a form and at rates useful to those who need it. The Commission believes that those who steadfastly resist connectivity will be perceived as unresponsive and will ultimately be considered as offering little value to their customers.

There is no doubt that increased connectivity creates greater vulnerability. Electronic access to vast amounts of data and critical infrastructure control is now possible from almost anywhere in the world. Networks are so complex and so widespread that the identity of everyone with 'access to the networks to which our systems are connected can no longer be known with any assurance. Moreover, although our classified data is obviously of great interest to our enemies, our communities depend on extensive data bases of unclassified information that if destroyed or damaged would cost billions to rebuild and could affect our ability to deploy and operate a flexible, capable force.

Protecting information transactions within the subinfrastructure or network enclaves controlled by the DoD and the Intelligence Community requires an approach to security in which information systems security is seen as part of a balanced mix that also includes personnel security, physical security and other security procedures. Protecting information transfers between our enclaves and the rest of the infrastructure where we cannot count on other types of security requires a more stringent form of information systems security. In addressing these issues, the Commission examined current threat information as well as policies and procedures now in place to protect against such threats. The Commission found our policies outdated, our strategies for obtaining necessary information systems security technology ineffective, and our general readiness in terms of awareness and training inadequate.

The Threat to Information and Information Systems

Thirty years ago, computer systems presented relatively simple security challenges. They were expensive, isolated in environmentally controlled facilities, and their use was an arcane art understood by few. Consequently, protecting them was relatively easy, a matter of controlling access to the computer room and clearing the small number of specialists who needed such access. As these systems evolved, their connectivity was extended, first by remote terminals and eventually by local and wide-area networks.

As size and price came down, microprocessors began to appear in the workplace, in homes, and eventually on the battlefield and embedded in weapon systems. What was once a collection of separate systems is now best understood as a single, multifaceted information infrastructure operated as a utility. To cope with this new reality, our paradigm for managing information security must also shift from developing security for each individual application, system, and network to developing security for subscribers within the worldwide utility, and from protecting the isolated systems we own to protecting systems that are connected and depend upon an infrastructure we neither own nor control.

Despite the enormous impact that could result from the compromise or destruction of our information systems, the Commission believes that there is little public understanding of the threat or of the consequences of attacks on our systems. One high-level official suggested that until there is a major information systems catastrophe, appreciation of the need for information systems security will remain weak. Attacks against information systems are becoming more aggressive, not only seeking access to confidential information, but also stealing and degrading service and destroying data.

Our paradigm for managing information security must also shift from developing security for each individual application, system, and network to developing security for subscribers within the worldwide utility.

The well-publicized Michaelangelo virus destroyed the information and applications software on the hard disks of the unwa y. In another example, a small program appeared on computers connected to the Internet. This program made copies of itself and sent the copies along to other computers on the network. The copies made copies in turn and sent them along, and the copies' copies made copies, and so on. In short order the network was so busy creating and sending copies of the program that if couldn't do anything else. Some of fhe computers were down for most of the following week, and the business enterprises, academicians, and government and private users were unable to use their computers for processing or to communicate among themselves.

Networks are already recognized as a battlefield of the future.

Networks are already recognized as a battlefield of the future. Information weapons will attack and defend at electronic speeds using strategies and tactics yet to be perfected. This technology is capable of deciding the outcomes of geopolitical crises without the firing of a single weapon. Our security policies and processes must protect our ability to conduct such infowars while denying our enemies that same advantage.

If, instead of attacking our military systems and data bases, an enemy attacked our unprotected civilian infrastructure, the economic and other results could be disastrous. Over 95 percent of Defense and Intelligence Community voice and data traffic uses the public phone system. The economic consequences alone of a successful attack on the phone system or the National Information Infrastructure would be significant.

The nine-hour failure of the AT&T public switch network in 1990, although the result of a reliability failure and not a planned attack, demonstrated how vulnerable we are. Of the 138 million long-distance and 800-number calls attempted, some 70 million were rejected by the faulty system. Many of those calls were business calls, and thefailure to connect cost those businesses directly due to orders not being placed and operations being delayed or halted altogether. There were indirect costs as well due to decreased efficiency and productivity. Airlines, hotels, and car rental companies lost reservations, Phoned catalog orders were not placed. Service companies could not support their customers.

The threat to our information and information systems is increasingly sophisticated, and comes from both insiders and outsiders. While improving the personnel security methods used to ascertain the trustworthiness of our people will reduce the insider threat, personnel security measures alone cannot be relied on to protect our information and information systems. Foreign intelligence services, including those of some of our "allies," are known to target US information systems and technologies, using techniques that can give them access to our information without ever coming into our work spaces or approaching our people. Some trends and specific incidents help indicate the scope of the information systems security challenge:

- Computer viruses are growing more common and more dangerous, and may be virtually undetectable by conventional antiviral software. Trojan horses, logic bombs and other malicious software are appearing on our systems, and require improved countermeasures and careful security procedures to defeat.

- Over 4,000 hacker attacks, ranging from attempted password cracking to trying to obtain control of the system, were detected on one government system during a single three month period: Some hackers advertise their services for seeking any information, including classified or sensitive information.

- Eighty-five percent of computer crime is committed by insiders with validated access to the systems and networks they abuse. Before being fired from a private firm, a disgruntled employee left a logic bomb in the company's personnel system that destroyed all personnel records. Careless insiders, ignoring security procedures, have inadvertently inserted viruses into DoD and Intelligence Community information systems.

- Increasingly cheaper and more powerful commercially available electronics put signals intelligence intercept and processing capabilities within the reach of the smallest countries and even drug traffickers. Targeting by signals intelligence of facsimile and data communications on land-based and satellite systems gives eavesdroppers access to international communications of US businesses, personal telephone calls of US troops stationed overseas, computer passwords, and other data.

Dated Policies

The Commission found a number of problems hindering the effectiveness of information systems security. Problems include ineffectual and conflicting policies, failed strategies for obtaining the necessary computer security technology, poor mechanisms for obtaining timely threat information, inherent systems vulnerabilities, lack of effective audit data reduction techniques, and accreditation processes that are far too slow. The Commission also believes that there is a need to improve the quality and number of information systems security professionals and to increase training and awareness programs for management and non-security personnel.

The policies and standards upon which the Defense and Intelligence Communities base information systems security services were developed when computers were physically and electronically isolated. As a result, policies and standards:

- Are not suitable for the networked world of today, having been based on stand-alone architectures where the security requirements imposed on one system had little or no impact on the security for another system.

- Were developed based on a philosophy of complete risk avoidance and so do not deal effectively with information systems security as part of a balanced mix of security countermeasures in protecting the confidentiality, integrity or availability of our information assets.

- Do not provide the flexibility needed to address the wide variations among systems in use today and planned for tomorrow.

- Do not differentiate between the security countermeasures needed within and among protected network enclaves and those needed when information must travel to and from less protected or unprotected parts of the infrastructure.

The policies and standards upon which . . . information systems security services [are based] were developed when computers were physically and electronically isolated.

The strategy for developing computer security software, hardware and other security technologies has not served us well.

- Are only beginning to combine computer science and public key cryptography effectively to protect information.
- Are not capable of responding in a timely manner to dynamically evolving information technology.

The Commission also found a profusion of policy formulation authorities all of whom are addressing essentially the same issues. The Community Counterintelligence and Security Countermeasures Office (CCISCMO) is responsible to the Director of Central Intelligence for information systems security policy and standards for the Intelligence Community. The DoD intelligence organizations must follow CCISCMO security policies, and all of the DoD must follow the security regulations promulgated by its chains of command up through the Office of the Secretary of Defense (OSD). The National Security Telecommunications and Information Systems Security Committee (NSTISSC) creates policies that overlap those of both the OSD and the CCISCMO with regard to national security information and extends its policy authority to other government departments and agencies not covered by DoD or DCI policies. The Office of Management and Budget casts its policies over all information systems security activities that expend tax dollars. The National Institute of Standards and Technology (NIST) is responsible for creating standards for the protection of unclassified but sensitive information. A result of these numerous policy authorities has been policies that, although similar, differ sufficiently to create inefficiencies and to cause implementation problems when organizations must coordinate their security protocols and procedures in order to interconnect.

Failed Strategies

In addition to dated polices and inadequate standards, the strategy for developing computer security software, hardware and other security technologies has not served us well. This strategy has been to encourage the private sector to design, develop, and manufacture products at their own expense. In return, the government promised that it would require these products be used in the systems and networks it acquired. However, the government did not follow through and buy these products when they became available. One reason is that the products suffered long delays waiting government approval and were consequently obsolete before being approved for use. In addition, these products are often too expensive and lack functionality comparable to state-of-the-art, nonsecure commercially available products. As a result, too few computer security products are available today and even fewer are in use.

These problems with obtaining commercial computer security products have been exacerbated by the government's failure to control and coordinate its own R&D programs. With each agency free to pursue its own R&D initiatives, some attractive lines of research have been neglected while there have been duplications of effort and products produced that are not readily interoperable with other computer security products. Moreover, research has been focused almost exclusively on providing protection to classified information and systems to the detriment of protecting unclassified information and our infrastructure assets.

The New Information Systems Security Reality

To meet the security needs of connected information systems using an in&structure not completely under our control, the Commission believes that there is a need for new information systems security policies and standards, new strategies for obtaining products, a more focused R&D program, and a better understanding of information security threats and vulnerabilities. Security requirements for evolving Defense and Intelligence Community information systems include:

- Providing the ability to securely pass classified information over public or open communication links or networks to authorized users.
- Resisting computer viruses and other malicious software, detecting and controlling penetration of networks, systems, applications and data bases by hackers, and surviving full scale infowar attacks.
- Ensuring the authenticity of electronic messages and preventing repudiation of their receipt.
- Keeping confidentiality and integrity of medical files, payroll records, and other sensitive but unclassified information.
- Protecting the privacy of personnel files and investigative dossiers as required by law.
- Providing confidentiality of the identities of personnel in sensitive assignments.
- Ensuring integrity in electronic payments to vendors and contractors.
- Ensuring the components of the information infrastructure are designed for the rapid detection of malicious activities and for the ready restoration of required services.
- Effectively managing and controlling access to information at any protection level on a global basis.

There is a need for new information systems security policies and standards . , . and a better understanding of information security *threats and vulnerabilities.*

Information Systems Security Policy for Tomorrow

The Commission believes that information systems security policy must better address current and future electronic environments. The network architecture of the future will comprise a seamless global web of unsecured electronic highways linked together to provide a common infrastructure operated as a utility. Subscribers will be a heterogeneous group of individuals and organizations tied into the network to communicate with each other and to obtain various services offered by some portion of the network. The Department of Defense and the Intelligence Community also will be subscribers and their networks will be subnets or "enclaves" within the larger infrastructure. Subscribers will use common standards in supplying and obtaining services, although security standards may vary from enclave to enclave. But security standards must permit subscribers to benefit from authorized connectivity and services provided by the infrastructure and other authorized subscribers.

A new investment strategy is needed to ensure that products are available that will ensure the availability and integrity of both classified and unclassified data.

The new policies must be network oriented, recognizing the need for coordination and cooperation between separate organizations and enclaves connected via the infrastructure. Policies must be sufficiently flexible to cover a wide range of systems and equipment. They must take into account threat, both from the insider and the outsider, and espouse a risk management philosophy in making security decisions. And given the knowledge that unclassified information can be just as important and is even more vulnerable than classified information, the new policies, strategies and standards must also ensure its protection. Information that has no requirement for confidentiality may still require protection to ensure that it is not illicitly modified or destroyed and is available when needed.

To alleviate the overlap, redundancy, and conflicts inherent in the existing policy formulation process, responsibility for generating the new policy must be given to a centralized security executive policy committee that represents both the Department of Defense and the Intelligence Community. Furthermore, in developing the new policy, representatives from outside these communities may need to be included to assure that a governmentwide perspective will be used.

The Commission recommends that policy formulation for information systems security be consolidated under a joint DoD/DCI security executive committee, and that the committee oversee development of a coherent network-oriented information systems security policy for the Department of Defense and the Intelligence Community that also could serve the entire government.

The Investment Strategy for Information Systems Security

A coherent set of policies is of no use if effective information systems security products are not available and programs can not be implemented that use them. Given the problems with the current strategies and programs, the Commission recommends a new approach based on a well-considered investment strategy that includes a more focused R&D program. It must obtain and use threat and vulnerability information in managing risk. And finally, it must result in a more robust, efficient, and responsive program for applying and managing information systems security in our systems and networks.

A new investment strategy is needed to ensure that products are available that will ensure the availability and integrity of both classified and unclassified data. Within an information systems enclave, security officials can rely on physical security to deny access to unauthorized users, personnel security to provide some assurance that those who do have access are trustworthy, and procedural security to manage access to and use of their subnets. However, protection against the outsider threat where the enclave connects to the outside infrastructure may require more stringent levels of protection. There must be assurance that, as information enters and leaves the enclave, highly protected data does not cross the boundary to lesser cleared subscribers and that information can flow into the enclave from the outside infrastruc-

ture without permitting access to unauthorized users or the introduction of malicious software.

The new strategy also must identify capabilities' and products that are needed to permit implementation of systems and networks providing various degrees of protection. Many in the private sector currently rely on insurance to protect against losses to hackers, criminals, and malicious software. The Commission expects that increased awareness of the economic risks inherent in connecting to or exchanging data with the information infrastructure will lead to an understanding that it is cheaper to protect information assets and information systems with technology than with insurance. This will, in turn, encourage the development of secure products by the private sector. Widespread use of such products will bring the cost down, permitting security to be used as a marketing discriminator as consumers will prefer secure products to those without security so long as the difference in price is not great. This process should result in the ready availability of affordable commercial off-the-shelf information systems and networks offering moderate levels of security assurance. However, the private sector is not expected to commercially develop those security products with the very high levels of assurance essential to some government systems and networks. Accordingly, the new investment strategy must provide for allocation of government funding to promote the development of high assurance products.

An investment strategy that allocates five to ten percent of the total cost of developing and operating information systems and networks [towards protecting them] is appropriate.

Computer security exists today that is deemed sufficient to permit connectivity within secure enclaves, as is the case at the CIA and the NSA. However, these same security countermeasures may not be considered sufficient when outside connections are established. Worse, interconnecting two secure enclaves that use different protection features may result in the failure of the security of both enclaves. Technology that would control information transfers across enclave borders is on the drawing boards and in the labs, but has not yet matured to a point where it can be used to protect connections between enclaves responsible for highly sensitive data and the unprotected infrastructure. Providing such technology at the earliest possible date must be a high priority for the new investment strategy

Adequate funding for information systems security is essential. In keeping with the understanding that the information infrastructure is an essential element of the national security structure, funds must be provided for the development of the technology needed to secure the infrastructure, both within secure enclaves and across the networks. Moreover, sufficient funding must be included in the agencies' and departments' budgets to ensure that program managers can buy computers, systems and networks that provide the security needed to protect the confidentiality, integrity and availability of information assets and information systems.

For the Department of Defense, the information infrastructure will be managed by the Defense Information Systems Agency (DISA), which must develop system and network security management capabilities as well as audit and alarm capabilities. The DISA is ideally situated to perform these functions and has created the Center for Information Systems Security to ensure the successful performance of its security responsibilities. The Center, although newly formed, has been doing an excellent job to date. Any necessary high assurance technology for securing information and information systems will be provided by the NSA. In reviewing the best practices of government and industry, the Commission finds that an investment strategy

that allocates five to ten percent of the total cost of developing and operating information systems and networks is appropriate and needed to ensure that those systems and networks are available when needed and safe to use. Smaller investment& are inadequate to achieve acceptable levels of risk. Larger investments are unrealistic given the expected budgetary environment facing our communities.

The Commission recommends that the Secretary of **Defense and the Director of Central Intelligence develop an information** systems **security investment strategy including an emphasis on commercial production of computer security components at affordable costs. The goal should be to use 5 to 10 percent of the costs of infrastructure development and operations to ensure availability and the confidentiality and integrity of our information assets.**

Research and Development-A Need to Consolidate

As part of implementing the new information systems security strategy, a carefully planned and well-managed research and development program is required. Information systems technology is evolving much faster than information systems **security** technology. The Defense and Intelligence **Communities must reassess, refocus and adequately fund our** information systems security research and development efforts to design and develop the highly technical products needed if our countermeasures are to provide **sufficient** defense to responsibly manage the risk to our information systems. However, the Commission has observed that there is no communitywide focal point for information systems security research and development. Each agency implements **the R&D activities needed for its own mission and, as a** result, there have been both duplication of effort and products made that **are** of very limited use.

A new emphasis on developing solutions for threats to the unclassified infrastructure also is needed.

In addition, research in the **DoD** and Intelligence Communities has been focused almost exclusively on providing solutions to protection of classified assets. As discussed earlier, the threats are changing, and targets in the future may well **be** found in the country's unclassified infrastructure power grid controls, transportation systems, the public switched networks, stock exchanges, and Federal Reserve monetary transfer system.

A new emphasis on developing solutions for threats to the unclassified infrastructure also is needed. The Commission believes that a **community**-wide **mechanism** to determine priorities for information systems security research and development of products is needed as part of the information systems security investment strategy.

The Commission recommends that:

a) Research and development programs be given high priority in creating the secure products which the DoD and the Intelligence Community need for **protection of their classified and unclassified information networks and systems.**

b) The Secretary of Defense and the Director of Central Intelligence assign the NSA as the executive agent for information systems security research and development for both classified and **unclassified information for the Department of Defense and the Intelligence Community.**

Infrastructure Security Management

Like other aspects of **information systems security, the** processes used **to** assess the security of our computers, systems and networks must evolve. With stand-alone systems, individual organizations not only own the information that is created, stored, and processed on their systems, they also own the systems themselves. In connected environments, information, resources, and processes are shared. Our methods for assessing the security of and deciding acceptable levels of risk must change. The existing processes are so **slow that products** and **systems are frequently obsolete before we are satisfied that they are safe to use.**

Infrastructure security managers must be able to detect when their net***works*** and connected systems are under **attack** and respond appropriately, If necessary it must be possible to perform triage and sever infected portions of the network or systems to save unaffected portions of the infrastructure. Hygiene measures must be implemented to prevent problems. Automated tools and security management workstations must be developed and **implemented** within our networks.

We must accommodate technology life cycles and provide for variations in the degrees of assurance required for differing applications and missions. Automated tools that support security administration (such as automatic monitoring and malidous code detection **and eradication)** and management **are** badly needed and must be developed as **part of the new strategy. Our** standards and processes should be compatible with international standards, processes and protocols that influence the technical design of the worldwide telecomputing infrastructure upon which our nation increasingly depends.

*Au**toma**ted tools that support security adtninis tra tion . . . and **manage-ment** are badly needed and must be developed as part of the new strategy.*

Auditing Infrastructure Utilization

Even though we place a high degree of reliance on the trustworthiness of cleared personnel given access to our systems, we must still be able to determine if any portions of the infrastructure are being abused, either by insiders or outsiders. This determination can be made by recording and analyzing the

information and control transactions that take place on the system, a process called auditing or, if conducted in real time, monitoring. Through auditing and monitoring, one can establish normal operating patterns, characterize trends, detect aberrations, and identify unusual activities. If insiders *or* outsiders are attempting to obtain, alter, or delete information to which they are not entitled, make unauthorized connections to the networks, or penetrate computer systems or applications, auditing and monitoring provides a means to detect their activities.

Despite the importance of auditing and monitoring, [we] currently are unable to conduct these activities effectively and efficiently.

However, despite the importance of auditing and monitoring, the Defense and Intelligence Communities currently are unable to conduct these activities effectively and efficiently. Too much data in too many forms is being collected. One hour of collected audit data requires an average of six hours of analysis for adequate review. Nor are audit capabilities user friendly. All too often audit records are left unopened or the audit capabilities are never activated. To increase our ability to detect unauthorized activity, the Defense and Intelligence Communities must develop common auditing and monitoring record formats and automated tools to assist in the reduction and analysis of these records. A focal point is needed for this activity. The DISA is the logical choice for executive agent. As the network manager for the DII, the DISA is already involved in the identification of requirements and the development and use of automated security analysis systems for networks.

The Commission recommends that the DISA be the executive agent for the Department of Defense and the Intelligence Community for development of operational security management tools for infrastructure operations, including more powerful audit reduction tools, automated tools for use in assessing the security of our networks and connected systems, and improving security management support technology.

Managing the Risk to Information Systems

The Commission believes that a central data base containing security-related events should be established. This data base would support the analysis of threats and vulnerabilities regarding information systems in the Defense and Intelligence Communities and will be useful in helping to frame risk management decisions. To ensure the most comprehensive information is available to risk management decision makers, contributing threat and incident information to the data base must be mandatory.

Because of the sensitivity of reporting vulnerabilities of, and attacks on information systems, the issue of whether to classify the database is contentious. If unclassified, it is feared that vulnerability information could be accessed and used by hackers, foreign intelligence agents and others to gain a better understanding of exploitable weaknesses. However, the use of a classified data base places restrictions on dissemination that would prevent use of vulnerability and threat information by those who need it to protect their systems.

The Commission recommends that the Secretary of Defense and the Director of Central Intelligence jointly establish and maintain an information systems security **threat** and **vulnerability data base. The data base should be available to all Defense and Intelligence Community organizations, including industry, and it must be mandatory that Defense and Intelligence Community organizations contribute all relevant information to it.**

Emergency Response-The Need for Help

The Commission recommends that in addition to creating **a** threat and **vulnerability** data base, a **central organization be identified to have the responsibility** of working with system managers to prevent and protect against attacks, to respond in a timely and effective manner if attacks occur, and to alert others when a problem is recognized. Such a capability should cooperate with the Computer Emergency Response Team (CERT) efforts now underway in private industry and academia and with other government **agencies. The** DoD has created the Automated Systems Security Incident Sup **port** Team (ASSIST) Program at the Defense Information Systems Agency to perform these functions. The Intelligence Community should support and rely on the DISA's ASSIST program and we recommend establishing the Program as executive agent for this function **governmentwide.**

A central organization [is needed]. . . to respond in a timely manner if attacks occur and to alert others when a problem is recognized.

The Commission recommends that the Secretary of Defense and Director of Central Intelligence appoint the DISA's ASSIST program as the executive agent for emergency response functions for the DoD and the Intelligence Community.

Information Systems Security Professionals

The Commission's final recommendation deals with our most important **information** systems security resource: people. The Commission recommends creation of a professional corps to execute the information systems security responsibilities. The Commission also recommends that a vigorous training program be established to provide for the professionalization needed by the local security professional while maintaining security consistency across our networked environment in both government and industry. The national **cryptologic** school is a good model for such professionalization training.

The information systems security problem is part of the larger security training and professionalization considerations discussed elsewhere in this report.

The Commission recommends the DoD and the Intelligence Community establish an information systems security professional development program as part of the overall development of security professionals.

Chapter 9.

The Cost of Security—An Elusive Target

No one has a good handle on what security really costs. Our accounting systems are not designed to collect security cost data and do not provide the analytic tools necessary to support *resource decision making.*

Understanding Security Costs

The total cost of security is a complex interweaving of direct charges and shared, hidden, and opportunity costs that cannot be captured by budget line items or data calls alone. The numbers do not tell the whole story and by themselves can be misleading. They do not account for the costs associated with inefficiency, excessive levels of protection, or lost opportunities. The Commission has tried to capture these less obvious costs, in addition to the conventional ones, in ik findings and recommendations in the belief that once identified, security costs can be better managed.

On the basis of information gathered in recent industry studies and our own analysis, it is clear that no one has a good handle on what security really costs. Our accounting systems are not designed to collect security cost data and do not provide the analytic tools necessary to support resource decision making. The Commission discovered early the difficulty of isolating discretionary or controllable security costs from those that are inherently part of the cost of doing business. Virtually every concern, public or private, buys some kind of security protection depending on the nature of the enterprise. To illustrate this point, figure 6 depicts various levels of security as a function of what is being protected. It shows how the classified world of security rests on a substantial underpinning of security resources. Even if there were no classified information or programs, there would still be basic security costs. We would fence off certain areas, put security police on flight lines, put locks on ammunition storage facilities and lock up expensive equipment. Figure 6 also depicts what we see as a building-block approach to security countermeasures in government and industry. The cost of doing business is represented in the four lower boxes. Each successive block requires additional protection and entails additional costs. The examples in each box are not all-inclusive but merely illustrative of the types of information being protected within each category.

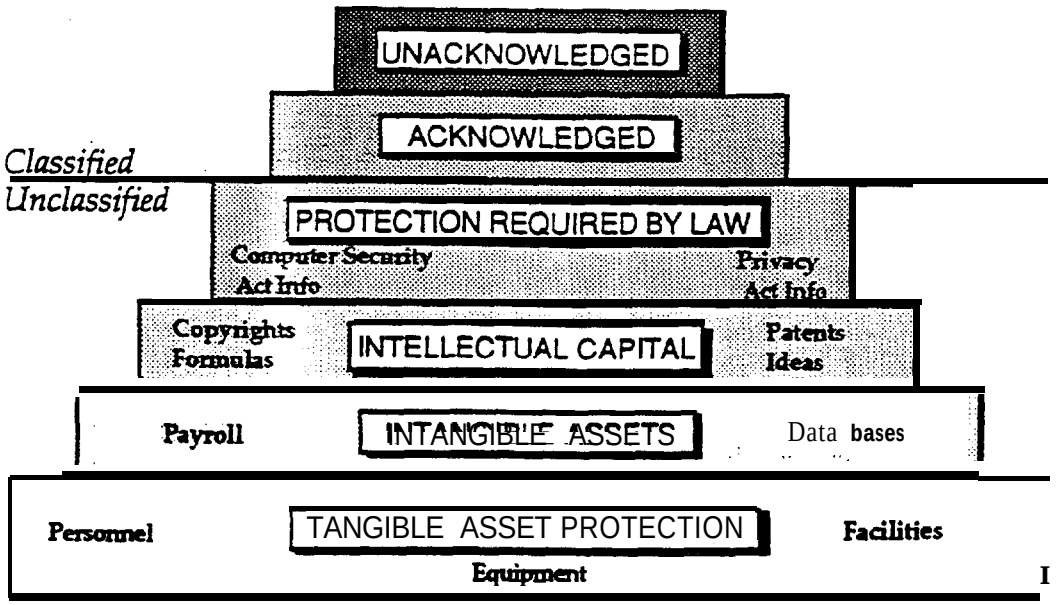


Figure 6. Protection by Program Type

SAP security costs can be exorbitant compared to acknowledged or collateral programs.

Costs in Black and White

Security costs can vary widely depending on the classification or the sensitivity of the work involved. The Commission has received some verifiable data points that can be used to gauge security costs in unclassified programs, acknowledged or collateral programs, and unacknowledged programs (especially those that use cover)[26]:

- In unclassified programs, direct security costs typically fall within the range of one-half to 1 percent of total operating costs (for government and industry).

- In acknowledged or collateral programs, direct security costs range from 1 percent to 3 percent of total operating costs.

- For unacknowledged programs, costs range considerably higher, from 3 percent to 10 percent of total operating costs. One SAP program manager estimated security costs could be as high as 40 percent of total operating costs. This estimate supports the widespread perception that SAP security costs can be exorbitant compared to acknowledged collateral programs.

Visible and Invisible Security Costs

The cost of security can be depicted as an iceberg having four facets. Two of the facets are visible and therefore more or less quantifiable. The other two are hidden below the waterline and, while difficult to measure, experience suggests they may be very large indeed.

As shown in figure 7, the visible facets of the iceberg are made up of direct and indirect security costs. Together they account for a small percent of the iceberg. Direct costs are quantifiable charges such as labor, equipment and

facilities. More difficult to quantify, but still visible, are indirect costs **that contractors typically** charge as overhead and general and **administrative (G&A) expenses. G&A** and **overhead charges are shared costs and may include, for** example, guards Who cover several program facilities or corporate security managers who service a number of programs.

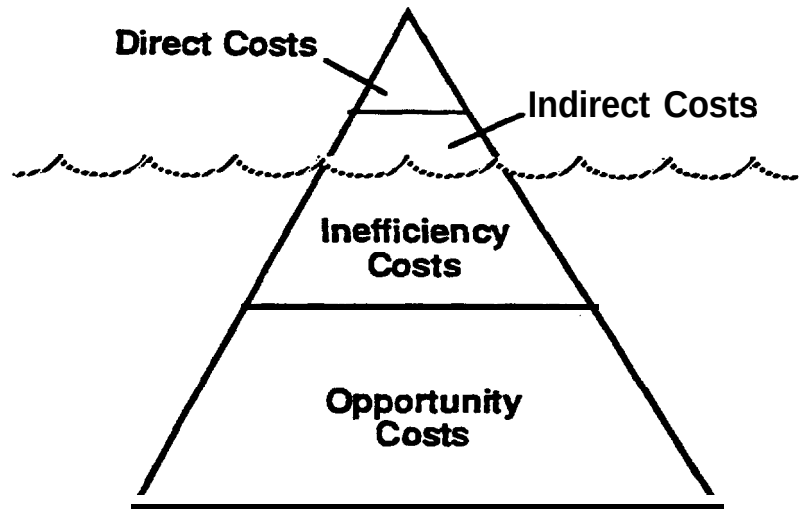


Figure 7. The Cost Iceberg

Below the waterline are difficult to quantify and comparatively large hidden costs, loosely defined as inefficiency and opportunity costs. The Commission believes that attacking these kinds of costs can yield near-term savings without degrading effectiveness:

As part of a contract to support a Special Access Program, a large defense firm on tk west coast must regularly visit a "sensitive" **activity in** *tk Boston area. Based on tk SAP security plan, which specifies that for cover teasons tk contractor must twt be associated with tk site,* **tk** *SAP program manager requires that contractor personnel traveling to Boston use circuitous routes by stopping at an intermediate location* **to** *change planes.*

Recently, another contractor needed to reassign 170 employees to work on a DZA contract. Despite all of their employees' clearances being on record in tk Intelligence Community's 4C clearance data base, DZA required new personal history statements from each person and readjudicated each case. After **six** *months,* **only 32** *people* **had been** *processed.*

With an eye toward the total cost of security, the Commission adopted the followingapproach:

- **Each of the subcommittees--threat, physical/technical, personnel, and information systems security-attempted to identify costs and investigated potential savings in its respective area.**

- The staff reviewed cost data in the National Foreign Intelligence Program (NFIP) and DoD budgets (excluding SAPs).

- The staff reviewed the just-completed final report of the NISP Resources Working Group, "Capturing Security Costs in Industry," as well as other recent industry cost surveys.

- The Commission held extensive discussions with industry (including three well-attended roundtable meetings) in addition to meeting with professional associations and public interest groups. We interviewed members of Congress and their staff, senior public officials, and working-level security officers in government and industry, all of whom addressed the security costs of doing business.

Establishing a coherent system to capture security costs is crucial to streamlining and cost reduction.

"There's No Way To Know How Much We're Spending on Security!"

This oft-heard declaration sums up the feeling of many managers, budget examiners, and members of Congress alike. Frustration in the Congress over the Intelligence Community's inability to justify its security expenditures in term of the changing threat led to a 0.5 percent reduction in the NFIP in FY 1993. There have been more recent calls for cost clarity and containment. Representative David Skaggs authored language in the FY 1994 Intelligence Authorization Act calling for the Director of Central Intelligence to report to the Intelligence Committees by 31 March 1994 on the cost of classifying documents and a plan for reducing classification-related costs. The Commission believes that establishing a coherent system to capture security costs is crucial to streamlining and cost reduction. While some progress is being made in the NFIP, the DoD, and the NISP, these disparate efforts are not well coordinated and are proceeding far too slowly to offer any hope that a uniform cost accounting methodology is achievable in time to meaningfully capture any of the Commission's cost-impacting recommendations.

The Commission recommends the creation of an ad hoc panel to create a common approach and budget framework for defining and tracking security costs in the DoD, the Intelligence Community, and industry.

Work to Date in the DoD

The DoD has embarked on an ambitious effort to capture security costs using Tactical Intelligence and Related Activities (TIARA) as a model. Under the auspices of the Assistant Secretary of Defense, C3I, the Intelligence Programs Support Group (ISPG) is at work on the so-called CI, SCM, and Related Activities (CISARA) initiative, which attempts to aggregate security costs that are not part of the NFIP.[27] A new data base incorporating CISARA as well as NFIP costs will make it possible to identify the cost of security throughout the DoD's Major Force Programs.

Intelligence Community Efforts

The Intelligence Community, under the auspices of the DCI's Community Management Staff (CMS), launched a parallel effort to capture security costs using methods compatible with the DoD's CISARA effort. For the first time, Joint DoD-NFIP Program and Planning Guidance was issued for the FY 1995-99 program build. Included as a part of a Common Budget Framework for programs in the Defense and Intelligence Communities were new security cost categories for NFIP and DoD programmers to follow in building and displaying resources allocated to security. In a follow-on directive signed by the Deputy Director of Central Intelligence, program managers were informed of the Commission's intent to use FY 1995 budget submissions as the primary source of security resource data. Unfortunately, the Commission did not receive usable resource data from all the NFIP programs. The data we did receive are incomplete, inconsistent and not coherently integrated into NFIP-wide cost estimates. As a consequence, the Commission has not been able to do much more than glimpse at the big security cost picture in the NFIP. The Commission's recommendation to create a uniform cost accounting methodology and tracking system should bring about the accuracy, uniformity, and responsiveness currently lacking in the Intelligence Community.

The Commission's recommendation to create a uniform cost accounting methodology and tracking system should bring about the accuracy, uniformity, and responsiveness currently lacking in the Intelligence Community.

Capturing Security *Costs* in Industry

There is a commonly held perception in industry that industry has been subjected to indiscriminate, inconsistent, and unnecessary security procedures at costs not commensurate with the risk of compromise or level of threat, The Commission concurs with the NISP's strategy to make security more effective and economical in industry by identifying:

- Cost efficiencies resulting from the development and application of baseline standards.
- Security standards for special activities or programs that exceed baseline standards and are not linked to demonstrable threats.
- Resource impacts of proposed changes in security standards and policies to aid risk-based decision-making.

Capturing security costs in government contracts is generally more difficult than capturing the other security costs, because in industry security costs are frequently carried as indirect charges. There is no separate requirement for industry to report these costs to the government. The NISP tasked a working group[28] to develop a measurement tool to determine the cost of security in both baseline and special programs standards and then to identify the most feasible system for monitoring continued data collection.

The NISP's effort to develop cost metrics led to several broad-scope industry surveys that tried to collect security cost data from government contracts. These surveys have had limited success for two primary reasons. First, they unsuccessfully attempted to capture indirect/imbedded costs, such as employee time spent completing personnel security questionnaires, conducting clearance determinations, and escorting visitors. Second, contractors are not required to respond to a survey conducted by a Federal agency. Thus, data

calls are unlikely to yield a sufficient number of responses for a representative sampling.

But the surveys have provided information, subsequently validated by independent auditors, that helps size the problem:

- Of the total costs billed to security for both collateral and special programs, 60 to 80 percent is directly attributable to security labor (wages, salaries, and benefits for security managers, document control personnel, guards, and couriers),

- An additional 10 to 30 percent of total security costs are for facility and equipment costs, including buildings, locks, alarms, and security containers.

- The remaining security costs are carried in overhead or G&A and not identifiable as security costs per se.

- Between 10 to 20 percent of contractors doing classified work for the government account for 60 to 80 percent of overall costs billed to security.

Since there are no common accounting practices for industrial security costs, there are huge variances in cost tracking systems used by contractors. The Commission believes that prescribing uniform accounting procedures for industry would be unworkable and unreasonably costly. An independent study by a government organization estimates that for its contractors alone, total start-up costs for a security cost reporting/tracking system would be about $12 million, with an annual recurring cost of about $8 million.

An alternative approach, offered by the NISP and endorsed by a consensus of government and industry security experts, is to focus on direct security labor and facility costs, since these categories constitute approximately 90 percent of costs billed to security by industry. Moreover, these costs can be extracted from contractors' existing accounting systems. Capturing the remaining 10 percent, which is no less important but harder to define, can be accomplished by sampling a small number of major defense firms to gauge trends across the entire business base. This strategy effectively divides costs traceable to security requirements into four categories:

- Routine security costs that would be incurred if there were no Federal Government contracts.

- Visible security costs usually associated with collateral programs and budgeted and controlled by the corporate security organization.

- Those contract-specific security costs for special activities and programs that are under the direct control of program or contract managers.

- Those imbedded costs not identifiable as direct labor that are related to security tasks and regulations and are accomplished by non-security employees and not recorded as security costs.

There is a commonly held perception in industry that industry has been subjected to indiscriminate, inconsistent, and unnecessary security procedures at costs not commensurate with the risk of compromise or level of threat.

The Commission endorses the joint government and industry strategy for capturing industrial security costs and recommends that this strategy be incorporated within the new accounting and budget framework for security.

Moving Towards Consistency

There are a number of recommendations where the cost-savings impact will be more gradual but nonetheless significant over the long term.

Capturing security costs in the DoD, the NFIP and industry consistently and at some reasonable level of detail is essential to baselining security expenditures. Unless all three define costs in a manner that lends itself to subsequent aggregation and analysis on similar program and budget cycles, it will not serve the needs of policymakers and risk managers at all levels who have to make sound security decisions in a resource-constrained environment.

Getting to the Bottom Line-The Payoff Is Long Term.. .

The Commission has made two types of cost-saving recommendations that will directly reduce costs. First, we have suggested ways to lower security costs (eliminating inefficiencies and excessive layers of protection) without degrading the effectiveness of protection. Second, the Commission has offered a number of specific proposals that will lessen the cost of security and reduce levels of protection without jeopardizing security by managing risk Because our focus has been on systemic problems, the kind that appear below the waterline on the **iceberg graphic, there are a** number of recommendations where the cost-savings impact will be more gradual but nonetheless significant over the long term. We have not been able to quantify the savings except in very rough terms:

- Overhauling the classification system will have cost-beneficial impacts on virtually every aspect of security. We will be able to integrate our information architectures and exchange people and ideas more efficiently, while protecting secrets effectively Moreover, if we classify less and declassify more, we will have to clear fewer people, buy fewer safes, and mount fewer guard posts.

- The personnel security system can be streamlined by mandating reciprocity, consolidating **functions** and **encouraging automation. Long-term savings will result from** merging investigative organizations for the Defense and Intelligence Communities, reducing investigative lag times, reducing the scope of the SSBI, mandating reciprocity of adjudications, consolidating DoD adjudicative centers, using industrial funding strategies for select security functions, consolidating security forms and establishing a personnel security questionnaire in electronic format.

- Revising physical security requirements will establish standards and ensure reciprocity. Costs can be reduced by eliminating routine industrial inspections, establishing *a* facility certification and registration system, reducing domestic TEMPEST requirements, discontinuing routine TSCM inspec-

tions, and maintaining central data bases for clearances for all of government and industry.

• Introducing effective oversight and disdpline into the security communities through the creation of the security executive committee and its supporting staff will reduce costs. So will streamlining the policy coordination mechanism by consolidating several committees and their supporting structures into one cohesive policy management structure.

• Taking full advantage of existing Defense and Intelligence Community training expertise and facilities by pooling resources and coordinating training initiatives is also a cost saver.

• Avoiding conflicting research and development programs will protect critical efforts that track changes in foreign intelligence threats as well as technology while freeing up resources for other priority needs.

. . . With Up-Front Costs in the Near Term

• Start-up costs for a new DoD-Intelligence Community badge system are estimated at $3 million. However, the benefits of increased efficiency and productivity savings suggest that the system could pay for itself in one year.

• Increasing our investment in information systems security will be expensive in the short run. However, the consequences of a security breakdown in this area are so critical and far-reaching, that committing additional resources is only prudent.

Increasing our investment in information systems security . . . is only prudent.

The Bottom Line

The Commission was not given a cost reduction target, and without being able to define costs precisely, meeting one would have been nearly impossible in any case. Nonetheless, the Commission believes that its recommendations can lead to net long-term savings. Furthermore, we believe there needs to be a sound resource strategy that:

• Links security countermeasures and costs to realistic threat assessments and risks.

• Provides a financial blueprint to guide resource allocation and establishes top-level policy direction and control over security expenditures.

The Commission recommends that the Secretary of Defense and the Director of Central Intelligence develop a long-term resource strategy for security.

Chapter 10.

Security Awareness, Training, and Education

The security education community has a critical role to play.

The success of the Commission's recommendations to improve security will depend in part on how well we can incorporate the concepts of risk management, standardization, reciprocity, accountability and a service mentality into the way we do business and into the fabric of the workforce. The security education community has a critical role to play in this process. The Commission is proposing a fundamental change in how we view and manage security. The concepts espoused demand greater responsibility from each individual. Management must be educated as to its responsibilities in the new environment and provided the tools to apply risk management effectively. Multidisciplinary security professionals will need to know the "why" as well as the "how" of security in order to move away from a compliance or checklist mentality toward a customer service philosophy. Employees will need to understand their critical role and feel that they have a personal stake in identifying and implementing the goals and objectives of their organization in protecting its assets.

The Present

The Defense and Intelligence Communities each have extensive training infrastructures in place focused primarily on their own needs. Interaction with respect to curricula and access to courses and material is, at best, informal among the various training facilities. Training criteria and requirements also vary between agencies and departments resulting in uneven performance levels of security officers. While the Commission recognizes the need for agency and department specific training and criteria, these independent efforts produce an inconsistent quality of training, result in a duplication of effort, and reinforce the parochial interpretation and implementation of national policy. The Commission has also found that despite the importance of security awareness, training, and education programs, these programs tend to be frequent and ready targets for budget cuts.

Training for the Future

The security system of the future will place greater demands on the entire workforce, but especially on the security professionals. The focus on creative, cost-effective solutions to security problems will require a thorough understanding of both the spirit and the letter of security policies, practices, and procedures. The security professionals will be asked to implement the changes that we are proposing and to provide the expert input needed to make risk management a viable reality The expertise and energy that molded

the present security system must be harnessed and directed to meet the challenges of the new security environment. **The standardization** of security **training** programs and development of career development tracks are important steps in this process and should be the primary goals of the training community. Uniformity in the skills and knowledge taught security professionals is needed not only to ensure the quality of work but also to foster a common understanding and implementation of security policies and procedures. The demonstrated need for reciprocity among government agencies and facilities argues strongly for the creation of a career program structure with defined levels of proficiency for security disciplines, professionalization criteria, cross-discipline training, rotational assignments, and opportunities for advancement.

As noted in the Information Systems Security Chapter of this report, no where is the need for standardization and professionalization more apparent than in information systems security Because of a lack of qualified personnel and a failure to provide adequate resources, many information systems security tasks are not being performed adequately. Too often critical security responsibilities are assigned as additional or ancillary duties. We have not identified all of the missions and functions to be performed by information systems security professionals and lack comprehensive, consistent training for information systems security officers; security engineers charged with developing secure systems, networks and security tools; and certifiers and accreditors who can assure us that our networks operate securely. Additionally, in technical areas like information systems security and TSCM, we should provide cross training between the defensive and offensive sides so that the lessons learned by one side can be of benefit to the other.

Building on the informal cooperation which already exists in some places, a formal partnership between the Defense and Intelligence Communities should be established to achieve these objectives and to realize cost efficiencies. Such a partnership would be based on the joint use of training facilities, the creation of common career fields and professionalization programs, and the consolidation of training management functions into an executive agent for security training. Working in cooperation with the agencies and departments, the executive agent would:

- Identify and catalog Defense and Intelligence Community requirements for security training and coordinate the development of courses to meet the requirements.
- Centralize training resources, facilitate community-wide access to existing training centers and products, and focus investment in training technology
- Implement curriculum review and instructor certification.
- Establish community course codes and create a central database of available training.
- Develop security professionalization criteria.

Uniformity in the skills and knowledge taught security professionals is needed not only to ensure the quality of work but also to foster a common understanding and implementation.

The Commission recommends that an executive agent for security training be appointed. This executive agent should standardize **security training, develop security professionalization criteria, encourage joint use** of **training facilities, and emphasize the development of information systems security training.**

A focused effort is also needed to educate management as to its security responsibilities and to teach principles of effective risk management and its application to **security** countermeasures. As the insider is cited as the major threat to the protection of information in government and industry today, managers must know how to spot troubled employees, how to help them, what resources are available, and how to use these resources to counter the insider threat.

Sensitizing employees to the continuing need for security will be a challenge in the post Cold War environment. Government and industry must *con*tinue to be made aware of their responsibilities in protecting our nation's assets. However, the Commission found that **all** too often security awareness **briefings,** while a cost-effective **way to reach the workforce, are viewed as bor**ing, irrelevant, and out-of-date. Presentations are often made **in** the same manner regardless of whether the **audience consists** of new recruits or senior management. Security awareness programs need to be tailored to the audience and refocused to provide current, specific examples of the diverse and multifaceted threats, emphasizing such topics as current counterintelligence issues and information systems security.

The Commission recommends that an increased emphasis be placed on developing and funding security education courses for management and up-to-date security awareness programs.

Chapter 11.

A Security Architecture for the Future

No substantive and long-term improvements can be achieved without a unifying structure to provide leadership, focus, and direction to the government security communities.

Throughout this report, we have identified problems that contribute to the complexity and cost of the security system and proposed recommendations for overcoming them. But as noted earlier, many of these problems are merely symptoms, not causes. The Commission unanimously believes that the fragmentation of the security policy structure is the prime cause of the problems now associated with security policies, practices, and procedures and that no substantive and long-term improvements can be achieved without a unifying structure to provide leadership, focus, and direction to the government security communities.

The Present

US Government security policies and practices have evolved in an ad hoc manner over the last four decades. Security policy is enunciated in a collection of documents (Executive Orders, National Security Decision Directives, National Security Directives, Presidential Decision Directives, legislation, and individual department or agency directives and orders) prepared at different times, by different people, in response to different requirements and events, not as part of a coherent planned effort. Additionally, the individual policy documents have been developed through consensus, an approach that is not only time consuming and slow to respond to change, but can also produce unsatisfactory results. Policy is often weakened in order to achieve consensus. As a result, the departments or agencies are allowed to ignore aspects of policy which they do not support, as has happened with the SSBI mandated by NSD 63, the new TEMPEST policy outlined in NSTISSI 7000, and the elimination of the two person rule.

This piecemeal approach to security policy has led to a decentralized policy structure in which multiple groups with different interests and authorities work independently of one another. Figure 8 represents some of the Defense and Intelligence Community groups that either have some role in the formulation of security policy or influence the process. Many of these groups have overlapping memberships and responsibilities, others operate in isolation, but all exact a cost in terms of time, energy, and efficiency.

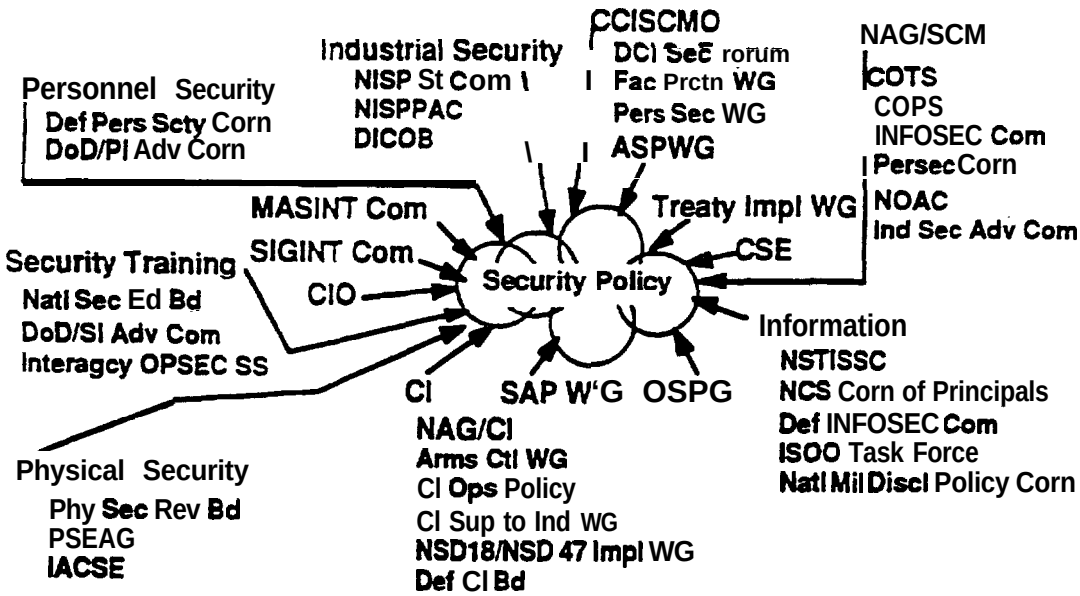


Figure 8. The Current Policy Structure

Each department or agency head is responsible for the appropriate implementation of security policy within his or her own organization. This decentralization presents its own unique set of challenges. The process is slow and some people never seem to get the word. Multiple agency originated implementation documents, while accommodating unique agency or department needs, also allow ample opportunity for the introduction of subtle changes, clarifications, reinterpretations, or additions that grow more pronounced with each iteration and can subvert efforts to standardize or update security policies and practices.

Oversight responsibility rests primarily with the department or agency heads and their respective Inspectors General. Although the Director of Central Intelligence has statutory authority for the protection of sources and methods, no comparable authority exists within the Defense Department where the Under Secretary of Defense (Policy), the Assistant Secretary of Defense (Command, Control, Communications and Intelligence), the defense agencies, services, and Joint and Unified Commands all have a responsibility for security policy. In addition, there is no effective mechanism to look across government to ensure that security policy is being implemented properly, if at all. Some personnel interviewed in the Defense and Intelligence Communities believe that there is, in fact, *no* penalty for noncompliance with security policy.

The Future

The problems inherent in this fragmented approach to security policy argue strongly for the creation of a security policy structure capable of pulling these disparate elements together and overcoming the bureaucracies' traditional resistance to innovation and change. The Commission recommends the establishment of a security executive committee to unify security policy

A security executive commit tee [would] unify security policy development; serve as a mechanism for coordination, dispute resolution, evaluation, and oversight; and provide a focal point for Congressional and public inquiries regarding security policy or its application.

development; serve as a mechanism for coordination, dispute resolution, evaluation, and oversight; and provide a focal point for Congressional and public inquiries regarding security policy or its application. Individual department heads would be able to request exceptions from general policies for their departments if deemed necessary.

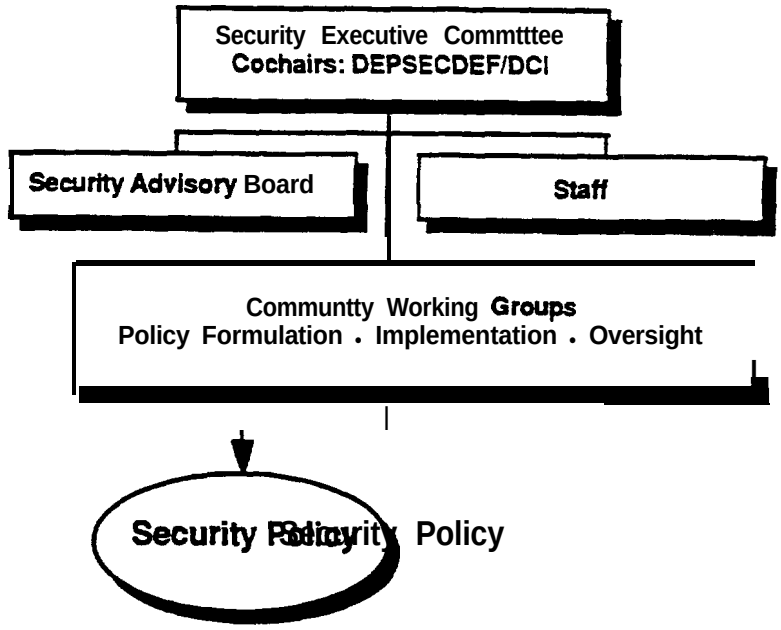


Figure 9. The Security Executive Committee

The [security advisory] board would act as a barometer for the committee to ensure that security policy and implementation is consistent with the overall goals of the government, such as openness, cost effectiveness, and fairness.

In view of the national security responsibilities assigned to the Department of Defense and the Director of Central Intelligence, we propose that the Secretary of Defense, or his designee, and the Director of Central Intelligence jointly chair the security executive committee. In recognition of the need to view security from a national perspective, the other permanent members would be the Deputy National Security Adviser, the Deputy Secretary of State, the Deputy Secretary of Treasury, the Deputy Secretary of Energy, the Deputy Secretary of Commerce, the Deputy Attorney General, the Chairman of the Joint Chiefs of Staff, and the Director of OMB. Other departments or agencies would be invited to attend committee meetings as required by the subject under discussion. In the Commission's view, the security executive committee should be established by the President under the auspices of the National Security Council.

The security executive committee would be assisted by a security advisory board composed of distinguished Americans who would provide a non-government and public interest perspective to security policy. The board would act as a barometer for the committee to ensure that security policy and implementation is consistent with the overall goals of the government, such as openness, cost effectiveness, and fairness.

A small permanent interagency staff would provide support for the security executive committee as required. Our concept would be to focus the staff on four functional areas: threat, policy development, implementation, and oversight. We would anticipate that the staff would facilitate, track, and expedite actions and would support whatever interagency committees and groups

might be required to ensure full community participation in the development and coordination of security policy and to effect horizontal integration of the individual security disciplines. The functions of existing staff structures, such as the Information Security Oversight Office (ISOO), the National Security Telecommunications and Information Systems Security Committee (NSTISSC) Executive Secretariat, and elements of the Community Counterintelligence and Security Countermeasures Office (CCISCMO) could be consolidated as subcommittees or in the permanent staff in order to streamline the structure and reinforce the concept of horizontal integration.

The security executive committee has a pivotal role in implementing the changes that we are proposing and in achieving our vision for the future. If created, it will facilitate the continuous and dynamic review of security policies, practices, and procedures needed to propel the government security communities into the new century. The scope and stature of its membership will give greater prominence to security and will combine the government security communities into a cohesive framework that can address the full range of security issues. It will monitor implementation to ensure that it is timely and consistent.

As an early goal, we believe the committee should enunciate a cohesive national level strategy for security which lays out goals and objectives and assigns responsibilities across govemment. The national scope of the strategy would ensure consistency and reciprocity among departments and agencies and recognize that security is a governmentwide responsibility.

The Commission recommends the establishment of a national level security policy committee to provide structure and coherence to US Government security policy, practices and procedures. The committee will:

1) Develop government security policy and standards.

2) Ensure long term and continuing implementation oversight.

3) Serve as an ombudsman to resolve disputes.

4) Monitor security resources expended and provide security program guidance.

As a first step, the Commission recommends that the Secretary of Defense and the Director of Central Intelligence immediately establish a committee to fulfill these functions for the Defense and Intelligence Communities.

Endnotes

1. The term "bigot" is said to have been coined during World War II, with reference to the controls on information sent TO GIBRALTAR, or TOGIB, reversed as BIGOT.

2. The Executive Order on classification allows Agency heads to create Special Access Programs to control access distribution and protection of particularly sensitive information. These include DoD Special Access Programs (SAPs), the DCI's Sensitive Compartmented Information Programs, and other information controlled by access lists. This includes CIA human source and operational information and Joint Chiefs of Staff war plans.

3. **Acquisition** programs for the protection of sensitive research, development, test and evaluation, or procurement activities in support of sensitive military and intelligence requirements.

   Intelligence programs for the protection of planning sensitive intelligence or counterintelligence **operations** or for the collection and exploitation of intelligence.

   Operations and Support programs for the protection of planning and executing sensitive military operations or providing sensitive support to non-DoD departments and agencies.

4. **Acknowledged** programs are those which are acknowledged to exist, although the public may not be **aware** of the Special Access Program. Details of the program are under special protective controls.

   Unacknowledged programs are those of which the mere existence of the Special Access Program is protected from all within government and industry who have not been determined to have a need-to-know. Knowledge of the existence of the program could endanger its success.

5. **The** current sentencing guidelines illustrate this confusion. The guidelines are based on the assumption, codified in the executive order on classified information, that the disclosure of Top Secret information will cause greater damage than the disclosure of Secret information. Under the existing guidelines a person will receive a more severe sentence for disclosing Top Secret than for disclosing Secret information. However, information protected as Secret SAP is often much more sensitive than "collateral" (i.e. non-SAP) Top Secret. Thus, the current sentencing guidelines could result **in a** person receiving a lighter sentence than is justified by the harm caused by the disclosure. The sentencing guidelines must be rewritten to reflect the classification system recommended by the Commission.

6. WNINTEL: Warning Notice- Intelligence Sources and Methods Involved

ORCON: Dissemination and Extraction of Information Controlled by Originator

NO FORN: Not Releasable to Foreign Nationals

REL: Authorized for Release to (Name of country(ies) or international organization) .

7. NO CONTRACT: Not Releasable to Contractors or Consultants

PROPIN: Caution- Proprietary Information Involved

8. Commissioner Lapham's remarks on secrecy agreements are contained in Appendix A.

9. It is not clear how many pages of information are involved. Some of these documents may consist of one or two pages, others may be much longer documents. This is important because the Department of Defense (DoD) and the Central Intelligence Agency (CIA), which together account for between 84 to 87 percent of those classification actions, report that an experienced reviewer is able to review approximately 200 pages of classified documents per day. (We are informed by DoD that during its review of MIA/POW documents an experienced reviewer was able to review about 200 pages of material per day, but that the average rate of declassification could be as low as 75 to 100 pages per person per day.) Based upon this data we estimate that an experienced reviewer, working an average of 240 days per year and reviewing an average of 200 pages per day could review 48,000 pages per year. Assuming an average of three pages per document or 18 million pages per year, it would require 375 reviewers to review a single year's product. Assuming an average grade of GS-12 (about $43,000 per year), this review would cost in excess of $16 million in direct salary costs. This does not take into account the additional administrative costs, for example, of finding the documents and all of the copies. Moreover, creating a government&de computer data base and entering all classification and declassification decisions will be a difficult and expensive undertaking..

10. 1993 Status Report on the Implementation of National Security Directive 47.

11. PERSEREC has proposed that the NAC be expanded to include all current NAC inquiries plus checks of other national automated databases. For example, the Title 31 data base maintained by the Treasury Department contains information on large and/or suspicious currency transactions that *merchants* and individuals are required to file with Treasury. These publicly available databases can provide investigators with leads concerning unexplained affluence and/or an important counterintelligence indicator that can be difficult to detect through traditional credit checks. Searches of these databases also can be automated such that investigators are notified only when certain thresholds are reached.

12. Based on OPM figures.

13. Commissioner Chayes's supplemental view on procedureal safeguards is contained in Appendix B.

14. Commissioner Lapham's remarks *on* the polygraph are contained in Appendix C.

15. "Polygraph" is Greek for "many writings," reflecting the multiple readings that are recorded simultaneously. The instrument-which was basically developed by 1949—measures physiological changes in response to questions.

16. NRO and CLA have approximately 40,000 contractors who have access and who have never been polygraphed.

17. The goals of the program are to:

    (a) provide an arsenal of valid and reliable security and applicant screening tests based on scientific evaluation of existing tests in comparison with new tests;

    (b) eliminate privacy-invading or personally offensive control questions;

    (c) evaluate a variety of sensors, transducers, and recording devices to establish the most effective and noninvasive physiological data collection systems;

    (d) develop algorithms that provide valid and reliable diagnostic results for each screening test that meets acceptable levels of validity;

    (e) develop countermeasure detection algorithms for all screening tests;

    (f) evaluate the effectiveness and utility of applicant screening tests;

    (g) determine the deterrent effects of the screening polygraph;

    (h) develop other tools for detecting deception that could be used in conjunction with or in place of the polygraph.

18. National Operations Security Doctrine, Interagency OPSEC Support Staff; January 1993.

19. Membership currently consists of representatives from the DoE, CIA, NSA, GSA, FBI, and the Secret Service.

20. The training of over 2200 government employees occurred from 1991 to 1993.

21. Examples include voting trusts proxies, special security agreements, board resolutions, and reciprocal agreements.

22. The Exon-Florio Amendment, Section 5021 of the Omnibus Trade and Competitiveness Act of 1988 (Pub. L. 100-418), enacted August 23,1988, permits the President to halt or reverse the acquisition of a US business by a foreign firm if he believes it would harm national security in a manner not adequately addressed by other federal laws. Executive Order No. 11858, as amended, 54 Fed. Reg. 779 (Dec. 28, 1988), delegates to the Interagency Committee on Foreign Investment in the United States (CFIUS) the authority to determine when a proposed transaction warrants review, investigations, and to submit recommendations to approve, limit, or halt transactions.

23. DoD Instruction 2015.4, dated 5 Nov 63, established the DoD Mutual Weapons Development Data Exchange Program and the Defense Development Exchange Program. Cooperative efforts expanded in 1976 with the creation of the International Professional Scientist and Engineer Program, followed by the Personnel Exchange Program.

24. A two-year US Army study of the Defense Data Exchange Program found that foreign governments successfully used a variety of overt and covert

collection methods to gain access to prohibited (non-releasable) classified and unclassified technologies, weapons systems, and programs.

25. The NDP establishes criteria and conditions that implement the security requirements contained in the Arms Export Control Act (AECA) and Executive Order 12356.

26. The terms "white" and "black" are also used to describe acknowledged and unacknowledged programs respectively. Although there is no standard definition of these terms in the security lexicon, in its broadest sense, "black" refers to not only to the aspect of covertness/clandestinity of a program but also to SAPs and other special activities that impose need-to-know or access controls beyond those normally provided for Top Secret, Secret, and Confidential information. Because these terms are not clearly defined and could be considered offensive to some, the Commission encourages the use of the terms "acknowledged" and "unacknowledged."

27. "Resource Estimates for Counterintelligence and Security Countermeasures," a study prepared for the Deputy Assistant Secretary of Defense, C3I (CI & SCM) by the Institute for Defense Analysis, September 1992 (updated December 1993)

28. "Capturing Security Costs in Industry: Final Report of the National Industrial Security Program Resources Working Group," December 1993.

Appendix A.

Statement of Commissioner Lapham on Secrecy Agreements

If this recommendation is adopted, it will inevitably gut the secrecy agreement that is currently required as a condition of CIA employment. The report suggests that the broad-form prepublication review provision contained in this agreement has no value, because the malicious will disregard it anyway and the conscientious can safely be held to a less broad requirement. I do not believe that the historical record supports this suggestion, and I am mindful of the fact that DCIs have repeatedly affirmed, with reference to the current agreement or ik predecessors, that the broad-form prepublication review provision is vital to the protection of intelligence sources and methods.

I do not believe that this recommendation should be adopted, if at all, without a much fuller accounting of the benefits that have been realized as a result of the obligations imposed by the CIA secrecy agreement, and the risks that would ensue if that agreement were to be modified in accordance with the recommendation.

Appendix B.

Statement of Commissioner Chayes on Procedural Safeguards

I support the conclusion, reached in the main text, that the procedural safeguards available to military personnel and DoD civilians facing denial or revocation of security clearances should be the same. I would go further, however, in urging that different treatment for DoD government and contractor personnel also be eliminated. Elementary fairness requires that we provide **uniform treatment** for both classes of people.

Reaching this state of affairs requires that we bridge the gap between the two sets of procedures currently in place. For many of the reasons stated in the main text, the formal trial-like procedures, using the Federal Rules of Evidence as a guide, and available to anyone who requests it, whether or not there are any factual disputes that need to be resolved represents procedural **overkill.** And while the process is perhaps more expensive, and time and labor intensive than necessary at the front end, it is less generous than it ought to be at the appeals stage.

A common set of procedures for both government and contractor personnel should require provision of a full and complete statement of the reasons for the proposed denial or revocation and a clear statement about the right to counsel at all stages of an appeal.

Appeal of the denial of an initial clearance should be decided upon a written response without an oral hearing. Broader rights should be provided in cases involving the revocation of a clearance or the denial of a higher clearance. In these cases, so long as the person claims there is a factual dispute, there should be the right to an informal hearing before a hearing officer who neither has any involvement in the issue nor is within the chain of command of those responsible for the clearance adjudication. The hearing should resemble an informal arbitration, with a transcript and the right to call and examine witnesses. The Federal Rules of Evidence should not be used and the process should be expected to take one day or less.

A second, written appeal should be available in all cases. A board established to review these appeals should not be limited to strict scope-of-review limits but should be free to take a fresh look at the case in reaching its decision.

Appendix C.

Statement of Commissioner Lapham on Polygraph

The Commission struggled hard to reach a consensus on issues relating to polygraph testing for personnel screening purposes. In the end, however, I decided to go my own way on these issues, and to prepare this separate statement of my views. I did so not because I disagree with all of the Commission's recommendations and conclusions-indeed, there are a number with which I agree--but mainly because I do not believe that the report contains an adequate or well-reasoned analysis of the issues, and because I believe that shortcoming impeaches even those recommendations and conclusions with which I do agree.

Polygraph testing is an obviously invasive procedure, the more so in screening contexts than in other applications. In the more typical setting there is a single factual issue that needs to be resolved, or some single event that is known to have happened and that is under investigation Therefore the scope of the test is apt to be narrow, as is the class of persons who may have some relevant information to provide. Screening polygraphs have no such natural limits. Almost by definition they affect larger classes of persons and sweep more widely for information. The goal is not to find out the truth about some event that is known to have happened, but rather to find out about the background and personal history of the person being examined. Given that purpose, multiple topics are within the field of inquiry, and the questions may range across an entire lifetime or a substantial period of years and may begin for example with the words "have you ever" or "within the last five years have you ever." The breadth of the inquiry is one reason why privacy interests are so deeply implicated by screening polygraphs, and especially by the full-scope tests that include the so-called "lifestyle questions."

There is also the matter of the surroundings in which the tests are conducted. The atmosphere is clinical. The chair is no more appealing than a dentist's chair. The technology is apt to be mysterious, and only one of the three machine-to-body connectors, the blood pressure cuff, is apt to be familiar. There is an underlying premise that something about to be said, or already said in a personal history statement, may be a lie. The examiner is a stranger, and the entire session, including the pretest interview and any posttest questioning, is being tape-recorded or videotaped and is destined to become a government record. Those circumstances are almost bound to make the test an unnerving and intimidating experience, even apart from the extent to which the questioning encroaches on privacy zones.

Privacy interests, however, are not the same thing as legitimate expectations of privacy. At least as I see it, any analysis of the polygraph procedure, like any analysis of other invasive techniques that are used to screen government personnel, such as drug-testing programs in which urine samples are

required to be given, must involve a balancing of such privacy expectations against the governmental interests that are at stake, and ultimately a determination as to whether the procedure is reasonable. My personal conclusion is that the procedure is reasonable. At least implicitly the Commission reached the same conclusion, but I get there by a different route.

Governmental interests and individual privacy expectations

At a threshold level, the analysis is pretty simple, and the balance is clearly in favor of the government. Not long ago, in 1988, the Supreme Court said that the nation's security depends in large measure on the reliability and trustworthiness of CL4 employees. That remark could just as well have been made with respect to others who occupy positions involving access to highly classified information. The self-evident point here is that the government has a compelling interest in assuring itself that such persons meet high standards. That interest necessitates a screening process. Individuals who seek intelligence agency positions, or other positions of equal trust, have every reason to understand and expect that such a process will be conducted, and that it will include a searching inquiry into their personal backgrounds. To be sure, there is room for disagreement about the appropriate scope of such inquiries, and as to the categories of information that are truly germane to the reliability and trustworthiness determinations that need to be made. In my opinion, however, so long as the inquiries stay within rational bounds and are carried out by lawful means, and with the consent of the persons affected, those persons can have no valid objections based on legitimate expectations of privacy.

Where the screening process entails a polygraph test, whether as a condition of initial or continued employment or as a condition of access, that fact is made known in advance, as are the topics to be covered. A decision to submit to the test is a matter of choice, requiring a voluntary consent by the person to be examined. In some cases that choice may be personally difficult, but then it is not the government's responsibility to make the screening process easy or painless. Nor can hard or difficult choices be equated with compulsion. A refusal to take a polygraph may have negative consequences, as for example the loss of a job opportunity at CIA *or* NSA, and there may be strong pressures to avoid those consequences, but this does not mean that a decision to take the test is forced or involuntary. While there are distinctions that can be made here between initial applicants for employment and persons who are already embarked on government or industry careers, and for whom therefore the pressures are undoubtedly greater, these distinctions are to some extent accommodated by the different test formats that are used and in any event it is still true that the tests are known-in-advance requirements, are conducted on a consensual basis, and not inconsistent with any fair expectations of privacy.

The relevance of the questions

However compelling the government's interest, the intentional collection of personal information unrelated to that interest, especially by invasive techniques, is not defensible. The issue here is therefore whether a rational link exists between the kinds of conduct that are probed by the "relevant" polygraph questions and the reliability and trustworthiness determinations that the government must make. In other words, the issue is whether these ques-

tions are "relevant" not just because they are so denominated in a polygraph test, but because they are tied to conduct about which the government has legitimate reason to be concerned and to inquire.

My own belief on this score is that, as the tests are currently structured, in both the full-scope format and the counterintelligence-scope format, all the relevant questions in the line-up deal with matters that are proper subjects of inquiry. Most of the controversy surrounds the so-called "lifestyle questions," which is the term commonly used to describe some of the questions that are asked when the test is given in the full-scope format, as it is to all applicants. for CIA and NSA employment.

I view the term "lifestyle questions" as an unfortunate misnomer. The flavor of the term is that these questions have only to do with personal matters that are none of the government's business. In fact, however, the questions deal with such matters as prior criminal conduct, illicit drug use, alcohol abuse, and any history of serious financial or mental health problems. These same subjects are matters of inquiry on personal history statement forms and associated forms, and during background investigations. If they were judged to be irrelevant, they should be declared out of bounds on all these fronts, not just on the polygraph front. As I see it, however, all these subjects can readily be linked to reliability and trustworthiness concerns, and to established adjudicative criteria. Indeed it is hard for me to imagine a credible screening process in which these subjects were not pursued.

At the same time, it is my opinion that some of the relevant questions, including some of the "lifestyle questions," as currently approved for use in screening polygraphs, are overly general and too broadly worded. As a consequence, as these questions are discussed between the examiner and the person to be examined during the pre-test interview, there is a high likelihood that personal information will be elicited, perhaps embarrassing information, that could have no value in any adjudicative decision. I would therefore favor an effort to rework some of the questions, so that they would have a sharper and more narrow focus at the outset, and so that there would be a lesser chance of eliciting irrelevant personal information. I would also like to see it become an explicit objective of polygraph examiners to minimize the incidental "take" of such irrelevant information. I believe these steps would shorten the tests, make them less intrusive, and reduce the number of retests that need to be given, all without any offsetting disadvantage.

Utility

I agree with the Commission's finding that polygraph testing has high utility as a personnel screening tool. The utility evidence is varied. It consists partly of data showing that large numbers of significant admissions are made during the interview phase of the procedure that takes place before the polygraph machine is ever activated and during the questioning that may follow after the machine is deactivated. There are also less tangible but nevertheless important utility considerations having to do with the deterrent effects of the procedure in relation to both applicants and employees, with the mutual trust engendered among employees by their common polygraph experience, and with the fact that the procedure is seen as eliminating the need for other personally invasive security safeguards, as for example random drug testing programs-

Without exception, the senior agency officials consulted by the Commission, having direct responsibility for polygraph screening programs, gave it as their opinion that these programs were the single most useful screening tool at their disposal, and were the linchpin of their peisonnel security efforts. Granting that these opinions hardly come from neutral sources, they are still worthy of respect and are made all the more significant when considered in the light of the Commission's recognition that personnel security is the most vital ingredient in any security system.

Validity

The question that lurks behind the utility evidence, particularly insofar as it consists of data showing success in the elicitation of admissions, is whether the procedure is otherwise a sham, and succeeds only because it is orchestrated in such a way as to make it appear to persons being examined that they have only two choices, one being to make admissions assuming they have something to admit and the other being to practice deception and be detected. In other words, as I see it, the fundamental validity issue is whether the promise of detection is an empty threat, and therefore whether the whole procedure is a trick, or whether within some range of probability the procedure can actually distinguish a true answer from a false answer. By endorsing various expert pronouncements that "The scientific validity of the polygraph [when used for personnel security purposes] is yet to be established, "the Commission appears to come down on the first side of this issue. As a consequence, when it goes on to recommend that polygraph screening programs be continued with certain modifications, the report apparently adopts the position that, even though the procedure employed by these programs is or may be invalid, the programs should be maintained in any event because they are useful. If the lack-of-validity premise of that position is accepted, the programs are likely to be discontinued despite their utility.

I am not so ready as the Commission to write off screening polygraphs as lacking in scientific validity, in part because the Commission never explains what it means by that term, and even if I were ready to do so, I still would not quickly jump ahead to the separate conclusion that polygraph testing has no validity as a personnel screening tool. What follows is my own non-expert conception of the problem.

A polygraph machine monitors, usually on three channels, physiological reactions that are produced by persons as they respond to questions that can only be answered yes or no. The reactions show up as tracings on charts. The machine is not difficult to operate. There is no real dispute that it does what it is designed to do-which again is only to monitor physiological reactions and make them visible in the form of chart tracings-and that it does so accurately

The validity problem arises not because the machine is fallible but rather because it requires an inference to derive some meaning from the charts, and because there are numerous important variables that bear on the correctness and strength of such an inference, the theoretical basis for which may itself be open to debate.

As the Commission notes in its report, there is no physiological reaction or combination of reactions that is known to be a unique earmark of lying or

deception. In isolation, therefore, any reaction or set of reactions to any one question is meaningless. So, for example, if I were placed on a polygraph machine and asked only the single question whether I was an agent of the foreign intelligence service of country X, and the truth was yes but my answer was no, the best polygraph examiner in the business could not make heads or tails of my physiological reactions to that question. It is only in relation to my reactions to other questions that the examiner could begin to make sense out of my reactions to the key "are you an agent" question, and have some basis for an inference that my answer to that question was false. That inference would proceed on the theory that I would have a heightened concern about the key question and therefore react more strongly to that question than to others that were asked for the purpose of eliciting reactions that could serve as points of comparison.

All polygraph tests rely on this essential theory The charts are diagnosed, or scored, and inferences thus drawn in favor of or against the persons being examined, by comparing the reactions to the relevant questions with the reactions to other questions. Different polygraph examiners, including CIA and NSA examiners, use different examination techniques, and different types of questions to elicit the reactions that are then compared with the reactions to the relevant questions in order to score the test. Each of the different methods has its champions, but nobody has ever discovered the magic formula. No matter which technique is used, no matter how skilled the examiner, and no matter what scoring system is applied, the resulting diagnosis may still be mistaken. If a truthful person is diagnosed as deceptive, the mistake is known as a "false positive." If a deceptive person is diagnosed as truthful, the mistake is known as a "false negative."

The accuracy and error rates of screening polygraphs are at best very difficult to estimate. The same is true in non-screening contexts, except in validity studies where mock crimes or some similar events are staged and the tests are then conducted in laboratory conditions, allowing the variables to be controlled. In such studies the guilt or innocence of the role-playing characters is known, although not to the polygraph examiner, and there is accordingly a stone tablet-a record of what is known in the business as "ground truth"-against which the examiner's conclusions can be crosschecked. Such tablets don't exist outside the laboratory, and even where they do exist, there is apt to be heated debate among experts about the design of the studies and about the extent to which their findings can be generalized.

None of this, however, leads *me* to believe that the use of polygraph testing for screening purposes is an unreasonable procedure. To say that polygraphy may not be an exact science is not at all to say that poiygraphers cannot reach credible and reasoned opinions, let alone that such opinions can be dismissed as wild guesses. We are not dealing here with a procedure in which an examiner simply hooks up a machine, looks at the charts, and delivers a verdict. We are dealing instead with a much more careful procedure, one in which both the relevant and other questions are previewed and discussed with the person to be examined, and in which the examiner then seeks to adjust the relevant questions so as to eliminate possible causes of high-stress reactions not attributable to deception. We are also dealing with a procedure in which equally careful efforts are made, following a run on the machine that does not produce a "clear chart," to again eliminate, by further adjustments in the relevant questions, any high-stress reactions to those questions that could have causes or explanations other than deception. At the end of the proce-

dure, if the high-stress reactions remain, there at a minimum is a rational basis for an inference that deception is the most probable cause of those reactions.

Where the Commission's report goes wrong, it seems to me, is in its apparent suggestion that the validity of polygraph testing is an all-or-nothing proposition. The sense of the report is that one or another of two propositions must be accepted---either the procedure is able to distinguish truth from deception with scientific accuracy, or it isn't able to distinguish anything at all.

If matters were this simple, the policy choices would be far easier than in fact they are. If polygraph testing produced results that were no better than random chance, say no better than the results that could be obtained by flipping coins, the arguments against it would be much stronger and might even be overwhelming, despite the utility evidence and the government's compelling interest in conducting an effective screening process. On the other hand, if polygraph testing results had the same degree of certainty as, say, the results of the testing of urine or blood samples, the arguments in favor of it would be much stronger, although for different reasons the technique would still be controversial. As it is, however, at least in my opinion, the reality is somewhere in between, probably much closer to the high end of the scale than to the coin-toss end but nevertheless at a point on the scale where there is some significant chance that opinions may be mistaken. The hard policy problem for any manager or adjudicator then becomes: how much credence can or should be given to such opinions, and who should bear the burden of the doubt, the government or the individual.

The Commission's report does not lay any of this out, but instead sidesteps and masks this policy problem by its treatment of polygraph validity as an all-or-nothing proposition, and leaves what I regard as a false impression both as to the state of the art today (the inference being that validity is zero) and as to the promise of research tomorrow (the inference being that something approaching absolute validity might be established.)

I am a strong supporter of further basic research, but I have also come to appreciate the challenge of designing high-yield research projects in this field, and I believe that any advances in knowledge will come slowly and in small increments. Again, in my view the opinion products of polygraph testing, assuming the competence of the examiner, are rational inferences either that a person is probably telling the truth or probably being deceptive, or perhaps that the results are too inconclusive to support an inference one way or the other. It may well be that a procedure that is so dependent on the competence of an examiner, and that deals in inferences about probabilities, could never meet exacting standards of scientific accuracy, no matter how extensive or well designed any future research projects might be.

If my conceptions are right, any DCI, Director of NSA, or Secretary of Defense who wishes to maintain polygraph screening programs, now or in the foreseeable future, will have to accept the uncertainty of accuracy rates, and the inevitability of some false positive outcomes, as facts of life. Likewise inevitable are some false negative outcomes. On that side the possibility that the polygraph can be "beaten," by physical countermeasures or otherwise, adds something, although nobody can say how much, to the accuracy rate uncertainty. Insofar as polygraph testing results may play a decisive role in connection with security approval decisions, these uncertainties mean that some deserving individuals will be screened out, and some undeserving indi-

viduals, conceivably even a trained foreign agent from whom we have the most to fear, will make their way through.

These uncertainties, however, need to be kept in perspective. While polygraph tests may not be scientifically exact, the other available means of investigating a person's background are anything but foolproof themselves. Personal history statements, personal interviews, and background investigations can be, and often are, carriers of information that is false, distorted, or misleading, purposely or otherwise, and record checks are not guaranteed to be reliable either. Even in the best of circumstances, the information derived. from these other sources does not meet, nor is it expected to meet, any scientific accuracy standards, and may be low-grade in terms of its value and credibility. If anything, polygraph testing is less open to being faulted on these grounds, particularly considering the fact that it so often leads to admissions that have undoubted reliability. Given a choice between two screening regimes, one of which would involve a personal history statement and the other traditional non-polygraph means of investigation, and the other of which would involve a personal history statement plus only polygraph testing, my guess is that CIA and NSA would vote for the second every time. However, there is no reason to make that choice, because better decisions are likely to be made when all sources of information are used in tandem.

Whether I am right or wrong in any of this, I do not think that any major policy shifts should be based on non-expert judgments concerning a set of issues that are as technically complex as the issues related to the validity of polygraph testing procedures used to screen personnel.

Recommendations of the Commission

I will turn now to the various recommendations contained in the Commission's report. Before doing so, however, I want to comment about one of the other statements in the Commission's report with which, I strongly disagree. In its catalogue of pro-polygraph arguments, the report includes an alleged argument relating to "cost-effectiveness," and goes on to say that both CIA and NSA present a good case that "[w]hen admissions made by a subject during a polygraph test result in a disqualification, these agencies are saved the considerable cost and time of conducting a background investigation. "As far as I know, neither CIA nor NSA has ever said that polygraph testing is conducted in order to save money. What they have said is that it makes more sense to conduct the testing, as they do, at the front end of the screening process, rather than as a last step in that process, because when things were done in the reverse sequence, as was formerly the case, too often the background investigation would be successfully completed only to find that the applicant made disqualifying admissions during the polygraph test. The real argument here is that polygraph testing often turns up information that background investigations do not. Cost effectiveness has nothing to do with whether such testing is conducted, only when it is conducted. Counting cost effectiveness as a pro-polygraph argument is incorrect and only serves to belittle the serious pro-polygraph position.

Scope. The Commission's first three recommendations relate to the scope of the relevant questions to be asked on screening polygraphs conducted by DOD and intelligence community agencies.

The first recommendation is that all such testing be limited to the so-called "C&scope" questions, except in the case of applicants seeking staff positions at CIA or NSA. As I understand it, this recommendation is principally aimed at the testing of contractor personnel, and specifically NSA contractor personnel and some CIA contractor personnel, who today are required to take the so-called "full-scope" tests. I agree with the recommendation. My reason for that agreement is that, as I see it, contractor personnel are in a somewhat different position, so far as concerns their legitimate expectations of privacy, than applicants for full-time staff positions at CIA or NSA. The latter are seeking careers that would give them continued and wide-ranging access to highly classified information over a long period. The former are apt to be persons who are already embarked on careers in industry, which they may well have undertaken without any reason to believe that their personal backgrounds would ultimately be the subject of searching inquiry by the government, and who in any event may have only less wide-ranging and only temporary access to highly classified information. In my view these considerations support the recommendation.

The second recommendation is that the testing of applicants for staff positions at CIA and NSA be limited to the so-called "CI-scope" questions plus questions about serious criminal conduct and recent drug use. The rationale is that the other questions currently asked on the so-called "full-scope" tests do not produce much useful information and therefore should be eliminated, producing a cost-free benefit in the form of a reduction in intrusiveness. In my judgment, as I have said, the other questions are not objectionable on relevance grounds, and I would be slow to discard them without a fuller cost-benefit breakout than I think the Commission has ever seen.

The third recommendation is that all reinvestigation polygraphs be limited to CI-scope questions. This recommendation would simply continue current practice.

Reciprocity. The Commission's fourth recommendation is that "the polygraph Should not serve as a bar to clearance reciprocity or to the exchange of classified or sensitive information." This recommendation is not explained in the report, and I am not sure what problem it is meant to correct, or what the correction would be.

Control questions. The fifth recommendation is a large mosaic of several ideas: that "the intrusiveness of control questions be minim&d;" that there be strict oversight to prevent abusive control questions; that information elicited by control questions not be kept in a permanent record unless it relates to criminal activity; and that appropriate compliance procedures be adopted and enforced.

The predicate of this recommendation is a finding in the report that "control questions are frequently identified as the most intrusive aspect of the polygraph." I do not agree with the finding, which I believe is based on several misconceptions, but I do agree that there is probably room to narrow the scope of control questions, just as I believe that there should be some narrowing of the relevant questions. So far as concerns the idea of keeping no permanent record of information elicited by control questions, I am very doubtful that this idea makes any sense, although it may deserve further study. If the idea were to be implemented, it presumably would require that the audiotape or videotape be edited. This would involve the partial destruction of these

records, even though one of the purposes for which they are kept is to assure their availability in the event of any complaint about misconduct or over-reaching by the examiner. Further, these records are held very closely, and I am unaware of any evidence that came before the Commission of any instance in which there was an improper release or any misuse of the kind of information to which the recommendation relates. While the recommendation calls for implementing procedures, it is impossible to know what sort of procedures the report might have in mind.

Over-reliance. The Commission's sixth recommendation is that "physiological reactions without admissions, to questions during a polygraph examination should not be used to disqualify individuals without efforts to independently resolve the issue of concern" This recommendation is low in clarity. What kinds of efforts would be required to "independently resolve the issue of concern," and what could happen if those efforts failed? Suppose there were two equally well qualified applicants for the same position, and the polygraph tests resulted in an examiner's opinion of probable deception in one case but not the other. Would that then mean that, absent some confirmation of the probable deception opinion, these results had to be ignored in making the decision as to which applicant to hire? The recommendation raises more questions than it answers, and provides no useful guidance.

Oversight. The seventh recommendation is that a new independent and external mechanism be established to investigate and track polygraph complaints. It is a given that polygraph programs should be subject to rigorous and effective oversight. This recommendation is made, however, without any real review of existing oversight structures, or any real effort to show how or why those structures might be inadequate, or any ***indication*** of how the new "mechanism" would be expected to operate. If the existing oversight is ineffective, obviously it should be improved. But within CIA, for example, there is already oversight within the Polygraph Section of The Office of Security, and there is also a special oversight panel (The Polygraph Complaint Oversight Board) which includes a representative of the Office of General Counsel and that was formed in mid-1992 for the explicit purpose of resolving polygraph-related complaints, not to mention the Inspector General's office. Surely any recommendation calling for additional oversight should be based on some showing, which the report does not contain, that these checks and safeguards are insufficient.

Standardization. The Commission's eighth recommendation is that "standards be developed to ensure consistency in the administration, application and quality control of screening polygraphs." There is already a trend in this direction, and I agree that further steps should be taken. I do not understand, for example, why the relevant questions, in whichever of the two basic formats the tests are given, should be different depending on which agency is conducting the test.

The different practices to which this recommendation relates, however, are overshadowed by circumstances that the Commission's report barely even mentions

Polygraph screening programs are not in effect, and have virtually no chance of being placed into effect, in parts of the government where highly sensitive national security information is handled on a steady basis. So, for example, no screening polygraphs are given to State Department employees

at any level, or to officials in the national security apparatus at the White House, or to members of the defense and intelligence committee staffs in the Congress, although many of these persons have access to much of the same information as intelligence agency employees, or to equally sensitive information. Even in DOD, the program has a very spotty application, if only because of the numerical limit on screening polygraphs imposed by the Congress. Among other things, high-ranking civilian employees are essentially exempt, and many high-ranking military personnel are also unlikely to be affected.

If the programs are truly important to the protection of national security information, the question that obviously waits to be asked is why the programs don't have more general coverage and acceptance. If they are needed in one place, why not in another? The Commission's report never asks this question. Instead it cites, and singles out for criticism, various differences in the ways in which polygraph screening programs are administered at CIA and NSA. These differences are small matters, however, compared to the double standard that exists by virtue of the fact that such programs are used in one form or another by both these agencies, and seen by both as indispensable security measures, but are not used in any form by other agencies whose personnel have access to the same or equally sensitive information. From a broad policy perspective, it is this double standard, not the much more minor differences cited by the Commission, that has real significance, because it points to a security system that taken as a whole is lacking in coherence and logic.

I am frankly at a loss to know where any of this leads, but there is at least a need to raise these considerations and make them part of the debate.

Certification. The Commission's next recommendation is that "certification of polygraph examiners under the auspices of a single entity should be mandatory" and that mandatory requirements for recertification also should be established." I do not know what this recommendation means. As I understand it, polygraph examiners who complete the training curriculums at the DOD Polygraph Institute or at the CIA polygraph school already receive certificates reflecting their successful completion of training programs approved by the American Polygraph Association. Further as I understand it, that Association views these programs as the finest of their kind in the country. I agree of course that superior training is a must, because competence and professionalism on the part of examiners are key elements in any polygraph program, but here again I have no basis to be critical of the way in which DOD or CIA polygraphers are trained, and the report provides no such basis.

National polygraph institute. The Commission's next recommendation is that "the CIA polygraph school be consolidated into the DOD Polygraph Institute to form a national polygraph institute that would conduct all training and certification of government polygraph examiners." This recommendation does not appear to have any cost cutting rationale, since none is mentioned in the report. Instead the stated objective is to "enhance the quality of polygraph training provided by the government." If such was the likely outcome, I would favor the recommendation, but here again the report provides no supporting reasons that point to such a likely outcome, and the recommendation has the feel of one that was made just for the sake of moving some furniture around.

Research. The Commission's last recommendation is that "a robust interagency-coordinated and centrally funded research program should be estab-

lished with DOD/PI as executive agent," and that this program "concentrate on the development of valid and reliable security and screening tests and standardize their use." I have already said that I am a strong supporter of further basic research: DOD/PI already conducts a broad research program, however, and I am not sure how the Commission would want to see this program redirected. Nor do I understand how it could be the function of any research program to "standardize" the use of polygraph tests. Only management decisions could have that result. Further, the wording of the recommendation suggests by implication that polygraph screening tests, as currently, administered, have no validity or reliability, and I do not agree with that implication, which may not have been intended.

Closing thoughts

I am not blind to the fact that screening polygraphs, for many people, are hateful experiences. The one such test that I took in my own life, which was one of the full-scope models, was certainly no picnic. It is only natural for people to think of themselves as patriotic, and fit to serve in government positions of trust should the opportunity to do so come along. All probably resent the idea that their honesty or integrity might be impugned by a polygraph examiner armed with a set of form questions and a strange technology. But there are higher stakes here, because mistakes can have fateful consequences for the country. Somewhere among us (no reference here of course to any members of the Commission) there are some bad apples. Others among us, whatever we may think of ourselves, do not meet the standards of reliability and trustworthiness that the government is entitled to set, and indeed must set if there are to be any personnel security controls at all rather than a system in which all comers are accepted, no questions asked. The standard-setting alone is a difficult job, and judgmental to the core. So is the sorting process. I end up believing that polygraph testing is a reasonable step in that process.

I am also well aware of the fact that polygraph testing has a high potential for abuse. There are few clear roadsigns here, however, and except in obvious cases, as for example if an examiner pursues unauthorized lines of inquiry, abuses are hard to define. I favor an effort to develop an agreed set of ethical guidelines, beyond any that exist today, that would apply to the conduct of screening polygraphs. I also favor the other steps to which I have referred in this statement, but in substantial part I do not favor the Commission's recommendations, and for that reason and the others I have already stated, I concluded that I could not join in the Commission's report.

Appendix D.

Acronyms

AECA	Arms Export Control Act
ASPP	Acquisition Systems Protection Program
ASPWG	Acquisition Systems Protection Working Group
ASSIST	Automated Systems Security Incident Support Team
C3I	Command, Control, Communications, and Intelligence
CCISCMO	Community Counterintelligence and Security Countermeasures Office
CCVS	Central Clearance Verification System
CERT	Committee of Emergency Response Team
a	Counterintelligence
CIA	Central Intelligence Agency
a 0	Central Imagery Office
CISARA	Counterintelligence, Security Countermeasures and Related Activities
CMS	Community Management Staff
COPS	Committee on Physical Security
COTS	Committee on Technical Security
CSE	Center for Security Evaluation
CTC	Counterterrorist Center
CTTA	Central TEMPEST Technical Authority
D a	Director of Central Intelligence
DCID	Director of Central Intelligence Directive
DCII	Defense Clearance Investigations Index
DDEP	Defense Development Exchange Program
DIA	Defense Intelligence Agency

DICOB	Defense Industrial Security Clearance Oversight Board
DII	Defense Information Infrastructure
DIS	Defense Investigative Service
DISA	Defense Information Systems Agency
DISCR	Defense Investigative Service Clearance Review Office
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDPI	Department of Defense Polygraph Institute
DoDSI	Department of Defense Security Institute
DoE	Department of Energy
ENTNAC	Entrance National Agency Check
EO	Executive Order
FBI	Federal Bureau of Investigation
FFRDC	Federally Funded Research and Development Center
FOIA	Freedom of Information Act
FOCI	Foreign Ownership Control and Influence
FORDTIS	Foreign Disclosure and Technical Information System
GAO	General Accounting Office
G&A.	General and Administrative
GOVIND	Government-Industry Restricted Information
GSA	General Services Administration
IACSE	Interagency Advisory Committee on Security Equipment
INFOSEC	Information Systems Security
IOSS	Interagency Operations Security Support Staff
ISOO	Information Security Oversight Office
ISM	Industrial Security Manual
ISPG	Intelligence Programs Support Group
LIMDIS	Limited Dissemination
MASINT	Measurement and Signature Intelligence
NAC	National Agency Check
NACI	National Agency Check with Inquiries

NAG/SCM	National **Advisory** Group/Security Countermeasures
NCS	National Communications System
NDP	National Disclosure Policy
NDPC	National Disclosure Policy Committee
NFIP	National Foreign Intelligence Program
NII	National Information Infrastructure
NISP	National Industrial Security Program
NISPPAC	National Industrial Security Program Policy Advisory committee
NIST	National Institute of Standards and Technology
NOAC	National Operational Security Advisory Committee
NOFORN	Not Releasable to Foreign Nationals
NPC	Nonproliferation Center
NRO	National Reconnaissance Office
NSA	National Security Agency
NSD	National Security Directives
NSDD	National Security Decision Directives
NSTISSC	National **Security** Telecommunications and Information systems **Security** committee
OADR	Originating Agency's Determination **Required**
OMB	**Office** of Management and Budget
OPM	Office of Personnel Management
OPSEC	operations security
ORCON	Dissemination and Extraction of Information Controlled by Originator
OSD	Office of the Secretary of Defense
OSPG	Overseas Security Policy Group
PERSEREC	Personnel Security Research and Evaluation Center
PEP	Personnel Exchange Program
PROPIN	Proprietary Information
PSEAG	Physical Security Equipment Action Group
PSWG	Personnel Security Working Group

R&D	Research and Development
RELTO	Releasable To
SAP	Special Access Program
SARF	Special Access Required Facility
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCM	Security Countermeasures
SIGINT	Signals Intelligence
SIOP	Single Integrated Operations Plan
SOR	Statement of Reasons
SPECAT	Special Category
SSA	Special Security Agreement
SSBI	Single Scope Background Investigation
SSII	Suitability and Security Investigations Index
TEMPEST	Transient Electromagnetic Pulse Emanation Standard
TIARA	Tactical Intelligence and Related Activities
TS	Top secret
TSCM	Technical Surveillance Countermeasures
USSS	United States Secret Service
WNINTEL	Waming Notice-Intelligence Sources and Methods Involved

Appendix E.

Acknowledgments

The Joint Security Commission is pleased to thank the following individuals and organizations for advice, counsel, and support in the preparation of its report:

AEGIS Research Corp.
Aerospace Corporation
Aerospace Industries Association
American Bar Association
American Civil Liirties Union
American Defense Preparedness Assoc.
American Federation of Government Employees
American Polygraph Association
American Society for Industrial Security
Analytical systems, Inc.
ARCA systems
Armed Forces Communications Assoc.
Arthur D. Little Corp.
AVCO/Textron Defense Systems
BDM International, Inc.
BETAC Corp.
Boeing
Bolt Barenek & Newman, Inc.
Booz-Allen & Hamilton, Advanced Decision Systems
Bristol-Myers Squibb Co.
BTG, Inc.
Central Imagery Office
Central Intelligence Agency
Charles Stark Draper Laboratory
CODEM Systems, Inc.
Communications Security Establishment of Canada
Computer Sciences Corporation
Contractor SAP/SAR Security Working Group
C. S. Draper Labs
Gay Research, Inc.
DCI Center for Security Evaluation
DCI Community Management Staff
DCI Counterintelligence Center
DCI Counterterrorist Center
DCI Non-Proliferation Center
Defense Information Systems Agency
Defense Intelligence Agency
Defense Investigative Service

Department of Energy
Department of Defense
Department of Justice
Department of State
DoD Polygraph Institute
Electronic Warfare Associates, Inc.
ESL
E-Systems, Inc.
Federal Bureau of Investigation
Federation of American Scientists
Galaxy Computer Services, Inc.
Dr. Robert Gates
GDE Systems, Inc.
General Dynamics
General Electric Co.
General Research Corp.
Grumman Corp.
GTE Government Systems
Hoffman-LaRoche, Inc.
Hughes Aircraft Co.
Hughes Information Technology Co.
IEEE
Information Security Oversight Office
Intelligence Programs Support Group
Department of Defense
International Information Integrity Inst.
ITT Aerospace
Joint Chiefs of Staff
Knoll Pharmaceuticals
Knollsman Instruments, Inc.
Litton Systems, Itek Optical
Lockheed Missiles and Space Company
Lockheed Sanders, Inc.
Logicon Ultrasystems, Inc.
Loral
Massachusetts Institute of Technology, Lincoln Labs
Martin Marietta
Mattel Toy Company
McDonnell-Douglas
MITRE Corp.
MRJ, Inc.
MVM Group, Inc.
Mystech Associates
National Classification Management Society, Inc.
National Communications System, Office of the Manager
National Federation of Federal Employees
National Institute of Standards and Technology
National Intellectual Property Law Inst.
National Reconnaissance Office
National Security Agency
National Security Archives
National Security Council
National Security Industrial Association
National Treasury Employees Union

Naval Criminal Investigative Service
Naval Post-Graduate School
Northrop
Office of Government Ethics
Office of Management and Budget
Office of the **Secretary** of Defense
Office Technology Assessment
PERSEREC
President's Foreign Intelligence Advisory Board
Rand Corporation
Raytheon Co.
SAIC
Dr. Roger Schell
Schering Plough
Secure Computing Corporation
Secureware
Security Affairs Support **Association**
Software Products **Association**
SRI International
TASC
Treasury Board of Canada
Trusted Information Systems
TRW
United Technology Corporation
US Air Force
US Army
US Atlantic **Command**
US Central Command
US Coast Guard
US House of Representatives
US Marine Corps
US Navy
US Secret Service
us senate
US Space Command
US Special **Operations Command**
UNISYS
United Technologies
Vitro Corp.
XEROX Special Information Systems